IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 December 2022, accepted 6 January 2023, date of publication 11 January 2023, date of current version 20 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3236254

RESEARCH ARTICLE

An IIoT-Based Approach to the Integrated Management of Machinery in the Construction Industry

OSCAR TORRES SANCHEZ[1,2], (Student Member, IEEE), DUARTE RAPOSO[3], ANDRÉ RODRIGUES[1,4], FERNANDO BOAVIDA[1,2], RADU MARCULESCU[5], (Fellow, IEEE), KONGYANG CHEN[6], AND JORGE SÁ SILVA[7], (Senior Member, IEEE)

[1]Centre of Informatics and Systems of the University of Coimbra (CISUC), 3030-290 Coimbra, Portugal
[2]Department of Informatics Engineering of the University of Coimbra, 3030-290 Coimbra, Portugal
[3]Instituto de Telecomunicações, 3810-193 Aveiro, Portugal
[4]Polytechnic of Coimbra, Coimbra Business School Research Centre (ISCAC), 3040-601 Coimbra, Portugal
[5]The University of Texas at Austin, Austin, TX 78712, USA
[6]Institute of Artificial Intelligence and Blockchain, Guangzhou University, Guangzhou 510006, China
[7]University of Coimbra, Institute for Systems Engineering and Computers (INESC), 3030-790 Coimbra, Portugal

Corresponding author: Oscar Torres Sanchez (otorres@dei.uc.pt)

The work presented in this paper was financed by Conduril, the UT Austin – Portugal Program / INESC TEC. It was also funded by Guangzhou Basic and Applied Basic Research Foundation(No. 202201010330, No. 202201020162) in the context of Alliance Joint Research and Publication Projects, and FCT - Foundation for Science and Technology, I.P./MCTES through national funds (PIDDAC), within the scope of CISUC RD Unit - UIDB/00326/2020 or project code UIDP/00326/2020.

ABSTRACT In recent years, considerable advances in connecting industrial equipment to the Internet allowed a higher level of operational efficiency, productivity, and automation. Nevertheless, the construction industry still presents challenging requirements, like long-distance wireless communication, interconnection of out-of- coverage areas, constant mobility of machinery, and support for legacy and proprietary systems. All these requirements pose different challenges when compared with traditional smart factory Industry 4.0 solutions. This paper discusses some of the current key questions regarding fleet management in the construction industry, identifies requirements for heavy-duty machinery, and proposes an Industrial Internet of Things (IIoT)-based solution for the integrated monitoring of such machinery. Also, it proposes and presents an open, innovative solution for the integrated management of non-standardized civil construction vehicle technologies. The developed prototype uses the J1939 protous and protocol to collect machinery status and Long-Range Wide Area Network (LoRaWAN) to communicate the monitored data. The solution was assessed at the construction site of the new port of Sines in Portugal. A detailed description of the proposed system is provided, along with information on trials and evaluation results regarding its performance. Additionally, the paper provides insights into open issues and challenges in this field and how our solution can contribute to overcoming them.

INDEX TERMS Industrial Internet of Things, management models, integrated industrial environments, industrial monitoring, industrial fleet management.

I. INTRODUCTION

Societies are paying increasing attention to Intelligent Transportation Systems (ITS). Intelligent fleet management systems have made it possible to develop services for energy, maintenance, risk, fuel, logistics, routing, and driver management [1], as well as reports on utilization, position, alerts, accidents, and operator interaction [2].

We are facing a new era of Connected Autonomous Vehicles (CAV) [3] that aims to provide users with an

The associate editor coordinating the review of this manuscript and approving it for publication was Stefano Scanzio.

excellent mobility experience. Autonomous mobility has been improved with approaches like Advanced Driver-Assistance System (ADAS) [4], Connected Autonomous Driving (CAD) [5], Unmanned Aerial Vehicle (UAV) and Unmanned Ground Vehicle (UGV) [6]. Furthermore, it foresees techniques for vehicle-user-city interaction [7], route management, intelligent traffic management, charging, and energy management. Lastly, remote diagnostics [8], intelligent public transport management, and safe and reliable road systems [6], among others, are emerging as the future of intelligent mobility. It can be anticipated that the new generations of 6G cellular networks will meet the requirements of the next generation ofCellular Vehicle-to-Everything (C-V2X) communication [6], [8]. The C-V2X concept contemplates Vehicle-to-Vehicle (V2V), Vehicle-to-Network (V2N), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) [8], [9].

Nevertheless, despite the significant advances in technology and communication of urban mobility systems, the field of off-road vehicles and civil construction machinery has yet to evolve. Vehicles such as excavators, backhoes, dredgers, pavers, compactors, dumpers, and loaders used in construction have limited technological innovation [10]. These vehicles typically use closed solutions with highly heterogeneous technology in what concerns types of machinery and brands, as well as low interoperability and standardization of communication protocols [11]. Furthermore, the construction industry often develops its activity under adverse conditions, characterized by noise, dust, instability, sudden movement, and low or no cellular coverage. So, in many cases, the use of next-generation communication technologies such as 5G and 6G cellular networks is neither feasible, nor practical [12]. These conditions dictate the use of long-range and low-bandwidth communication network alternatives such as LoRaWAN, SigFox, or nNarrowBand Internet of Things (NB-IoT) [13]. Finally, standardized monitoring protocols, such as CAN bus 1 Mbps and RS-485 2 Mbps for the physical layer or J1939 and J1758 in higher layers, are limited by their low capacity and bandwidth [14]. These problems limit the ability to integrate intelligence into machinery monitoring processes, preventing the construction industry from evolving toward Industry 4.0 or 5.0 concepts [15].

To overcome these major issues and challenges, IoT-based approaches can provide preventive maintenance, real-time observation and monitoring, construction and site management, operator and human resources monitoring, accident prevention alarms, and operating cost reduction. However, there is still substantial ground to cover in what concerns the adoption of IoT-based approaches, namely the lack of robustness, interoperability, limited connectivity, reduced industry standardization, security and encryption methods, data management issues, high data accuracy requirements, the complexity of use, compactness, and longevity.

This article presents a novel architecture for monitoring construction machinery through IoT devices. The proposed solution considers the construction industry requirements and allows to monitor and manage data from off-road vehicles. Furthermore, the presented approach enables the monitoring legacy and current systems using intelligent Industrial IoT (IIoT) solutions. The contributions of this paper are as follows:

- the identification of the requirements for the use of IIoT in the construction industry, comprising monitoring, communication technologies, and management models;
- a new solution for real-time integrated monitoring of construction machinery;
- a detailed description of the implementation of the proposed solution, along with information on real-world trials using this platform;
- identification and discussion of open issues and challenges for IIoT management.
- To the best of our knowledge, this is the first paper to present an open, integrated solution for heterogeneous and/or non-standardized, off-road civil construction vehicle technologies. The proposed solution is a first step to developing an integrated management platform for Industrial IoT.

The remainder of the paper is structured as follows: Section II analyzes existing, related work, concerning IoT management models for industrial environments. This is followed by the identification of requirements for IIoT management in the construction industry, in Section III. Section IV describes the proposed solution. Trials and evaluation results are presented in section V. Section VI concludes the paper by discussing open challenges and identifying guidelines for future work.

II. RELATED WORK

This section presents an overview of existing protocols and solutions for network management in IIoT. Sub-section A provides background on IIoT management, including considerations for network management of industrial devices and embedded devices, main challenges, and a brief overview of IoT network management protocols. Sub-section B compares management approaches for IIoT, including some solutions targeting the construction industry.

A. IIoT MANAGEMENT BACKGROUND

IoT-based approaches for monitoring the construction industry machinery must consider the interaction between IoT devices, data management platforms, and internal machine monitoring protocols. To realize intelligent monitoring using IoT as a basis, it is necessary to consider essential aspects of network management, thus obtaining solutions that add features to the already established techniques for monitoring machine parameters.

Management is one of the most critical aspects of ensuring proper network operation because it enables monitoring network status and applying corrective measures when required. In addition, it allows fault detection, parameter setting, status and performance data collection, and behavior control. Network management relies on protocols that support the

exchange of management data between the elements in the network.

It is essential that management systems support a variety of communication technologies. For example, Bluetooth [16], Wifi [17], [18], LTE [19], Long-Range Wide Area Network (LoRaWAN) [20], Sigfox [21], NB-IoT [22], and Zigbee [23] are commonly used in IoT industrial environments. Additionally, the current trend is to integrate IoT with 5G systems [24]. Although this variety of technologies has advantages, it also poses some challenges to management systems [25], [26].

One of the biggest challenges in managing IoT systems comes from designing and implementing solutions that can deal with heterogeneity. To address this, over the years, various network management protocols have been released. Some of the protocols for managing IoT environments include Simple Network Management Protocol (SNMP) [27], LowPAN Network Management Protocol (LNMP), Device Management (DM), Lightweight Machine to Machine (LwM2M) [28], Network Configuration Protocol (NETCONF) [29], Representational State Transfer Configuration Protocol (RESTCONF) [30], and CoAP Management Interface (CoMI) [31]. Industrial IoT management typically resorts to well-known protocols, like:

- **LwM2M DM:** A protocol developed by the Open Mobile Alliance (OMA) for machine-to-machine communications in IoT environments. Although LwM2M was developed as a management protocol [28], it is commonly used for telemetry, thus supporting two significant functionalities: data communication and device management. Furthermore, LwM2M can transport practical protocols for Industrial environments, namely, TCP over TLS, UDP over DTLS, SMS, and Non-IP (LTE-M, LoRaWAN, and NB-IoT) [25].
- **LNMP:** A protocol developed for working with the IPv6 Low Power Wireless Personal Area Network (6LoWPAN) standard, based on the SNMP management protocol. LNMP's architecture consists of two different management approaches for devices: the operational architecture, and the informational architecture. The operational management architecture seeks to discover end devices, coordinators, and gateways, and to support device monitoring. On the other hand, the informational management architecture is concerned with defining management information bases for the various layers of the 6LoWPAN network stack [25].
- **Message Queue Telemetry Transport (MQTT):** A lightweight messaging protocol for IoT environments and telemetry services. MQTT is not a management protocol [25], but it has been used for management in several commercial solutions like Amazon Web Services, Microsoft Azure, Google Cloud, to name a few. MQTT uses the publish-subscribe paradigm implemented on top of TCP or other transport protocols. The protocol is supported by three main entities, namely the publisher, the subscriber, and the broker. LwM2M is the prevailing protocol in management systems for constrained devices. Nevertheless, MQTT is widely accepted and used, as it demonstrated that it can be easily and efficiently used in management solutions for industrial environments, although it has not been designed for that purpose [25].

B. IIoT MANAGEMENT SOLUTIONS

Over the years, several models, protocols, and frameworks have been designed to manage devices in a network. However, the landscape has changed since the emergence of constrained IoT devices, which require protocols and frameworks that consider low power consumption, processing, and memory limitations. In addition, IoT device management in industrial scenarios is even more challenging due to adverse communication conditions. Within the literature, several papers have addressed management for IoT-based approaches for industrial environments and some specifically in construction industry scenarios [25]. Considering the background presented in sub-section A, this sub-section analyzes work that explores IoT approaches for integrated management environments.

In [26], the authors propose an architecture to monitor industrial processes using wireless Sensor Networks (WSN). The approach seeks to enhance the management of WSN and overcome dependability issues caused by problem-specific or non-standardized IoT networks. Additionally, this architecture was used to conduct two new studies on fault detection and security. The first study aims at detecting operation anomalies originated in firmware and hardware through parameters like high temperature, buffer overflow attacks, SPI faults, and undervoltage [32]. The second study explores vulnerabilities in WirelessHART, and uses the One-Class Support Vector Machines machine learning approach to detect attacks like jamming and collision [23]. Although these studies use a sound approach based on WSN and Industrial monitoring, there is still need to address new features and technologies in the vast spectrum of the requirements of industrial management based on IIoT.

Codeluppi [33] developed a modular IoT management platform called VegIoT to monitor and analyze garden data such as air, soil humidity, and temperature. The architecture implements an Internet-enabled Home Node (HN) and a mobile application to visualize the status of the parameters. This low-cost, modular, and energy-efficient platform was used in a Smart Agriculture environment, and exciting techniques were used to implement LoRaWAN as long-range data communication. However, the paper fails to adequately explain several aspects of the design of the proposed modular management approach.

Killen [34] proposes an IoT architecture for predictive maintenance for fleet management. This work includes a semi-supervised machine-learning model to improve sensor selection. The architecture targets transport monitoring and takes advantage of the J1939 protocol used in most heavy

TABLE 1. Comparison of management approaches for Industrial Internet of Things.

Name	Date	Challenges	Benefits	Disadvantages	IIoT Management Elements (Fault, Configuration, Accounting, Performance, Security)
Industrial IoT monitoring: Technologies and architecture proposal [26]	2018	Process-automation for problem specific monitoring	Industrial management standards Prototyping	Reliability and security concerns No hardware perspective	Fault
Securing WirelessHART: Monitoring, exploring and detecting new vulnerabilities [23]	2018	Intrusion detection evaluation	Security evaluation for common attacks	Focused on WirelessHART	Security
Security and Fault Detection in In-node components of IIoT Constrained Devices [32]	2019	Detect firmaware and hardware anomalies.	Machine learning techniques	Does not consider node's performance	Fault, Configuration,Security
VegIoT Garden: A modular IoT Management Platform for Urban Vegetable Garden [33]	2019	IoT platform for Smart Agriculture	Modular IoT platform Short and Long Range Real Scenario	Security not evaluated	Fault,Performance
IoT-based predictive maintenance for fleet management [34]	2019	Predictive maintenance	J1939 support Semi supervised ML over J1939	No real scenarios evaluation. No variety of network integrators	Fault, Configuration
Trust Management in Industrial Internet of Things [35]	2020	Trust management model	Model for Security and privacy Hybrid network for industrial rules	No cryptography concerns	Security, Accounting
Scalable Fleet Monitoring and Visualization for Smart Machine Maintenance and Industrial IoT Applications [36]	2020	Scalable fleet monitoring	Smart maintenance Dynamic fleet monitoring Specific IIoT requirements	Lack of evaluation of predictive maintenance	Fault, Configuration
Vulnerabilities and Security Threats for IoT in Transportation and Fleet Management [37]	2020	Comparative analysis of vulnerabilities and threats	Roles' description in IIoT context Quantitative analysis on fleet management	Insufficient explanation of tool conditions	Security
Low-cost internet of things(IoT) for monitoring and optimising mining small-scale trucks and surface mining shovels [38]	2021	Monitor performance of minning small-scale trucks	Automate the management data collection Real scenario evaluation	Limited positional information Limited driver alerts	Fault, configuration
An Automatic Overloaded Vehicle Monitoring and Prevention System using IoT [39]	2021	Monitor and prevention heavy vehicles ovearloding	Avoid movement of overloaded vehicles Inclination monitoring	No real scenarios test	Fault
Design and Development of the Smart Object for the IoT-enabled Smart Warehouse [40]	2022	IoT-based smart object for monitoring	Smart objects, and smart hand pallet truck Raspberry Pi for data processing	No real scenario results	Fault

transports. The system performs lightweight data analytics based on a selected J1939 sensor chosen by an ML model. This reduces the amount of data to analyze. However, the authors fail to prove that this is better than collecting the data from all the sensors using MQTT to have a complete view of the system.

Boudagdigue [35] developed a trust management model for IIoT devices in the automobile industry. The model seeks to provide security and privacy to IIoT devices and their industrial processes. In addition to security, this work implicitly introduced accounting, through permission and access control. However, it does not include crucial security aspects like cryptography to protect user communication.

In [36], Scalable Fleet Monitoring and Visualization for Smart Machine Maintenance and Industrial IoT Applications are presented. This architecture combines scalable fleet monitoring with predictive maintenance. Its dynamic dashboard application for fleet monitoring and visualization helps to evaluate specific IIoT application requirements. However, the paper fails to explain the predictive maintenance process and the metrics used in more detail

Zahra [37] presents a comparative analysis of IoT's vulnerabilities and security threats and their mitigation strategies in transportation and fleet management. The authors mainly try to classify the existing strategies based on their underlying principles: physical security, gadget management, network services, weak passwords, outdated components, privacy protection, and overhaul mechanisms.

Aguirre [38] shows the results obtained in a real scenario implementation in Chile. The work addresses low-cost IoT monitoring and optimizing mining on small-scale trucks and surface mining shovels. The experiences center on evaluating how the implementation optimizes and automates the management information collection process. The model is also used to improve operational decision-making through IoT devices. However, the presented solution has problems with the positional information collected by the Global Navigation Satellite System (GNSS) functions. Furthermore, it does not integrate alerts for drivers and alternatives for network connections besides mobile networks.

Praveena [39] automatically detects overloaded vehicles to prevent failures using IoT sensors. To avoid the operation of overloaded vehicles, the system cuts the battery power, preventing ignition. Finally, Silapunt [40] designed and developed intelligent objects and a smart hand pallet truck. The work is focused on goods identification using UHF RFID, processed through a Raspberry Pi, and providing an intuitive Graphical User Interface. Nevertheless, the work does not adequately explain the architecture used to transport the data from the collection point to the GUI.

Table 1 summarizes the main characteristics of the various approaches presented above, highlighting the advantages, disadvantages, and management aspects considered in each work.

The IIoT-based approach presented herein considers a management platform to monitor a large variety of equipment

used in the construction industry, provides secure access to data, and supports intelligent data analysis. Furthermore, it deals with issues such as using several protocols and technologies like J1939 and others, fleet and driver management, and integration of constrained devices for internal monitoring of internal machinery. In addition, this IIoT platform resorts to long-range wireless technologies providing communication to devices in adverse conditions.

The following section provides an overview of the requirements of IIoT management for the construction industry.

III. IIoT REQUIREMENTS FOR THE CONSTRUCTION INDUSTRY

The IIoT construction industry requirements addressed in the current section consider the following aspects: wired and wireless industrial monitoring (sub-section A), wireless communication technologies and services (sub-section B), and network management models for integrated IIoT environments (sub-section C).

A. INDUSTRIAL MONITORING

Many construction companies are still using wired technologies to implement monitoring of their machinery. Wired technologies are reliable and largely proven. However, they are costly, not easy to install, and cannot meet several IIoT and Industry 4.0 requirements. Nowadays, wireless sensor networks and IoT are driving the change to wireless communications in the monitoring of industrial processes [26]. On the other hand, industrial WSNs (IWSN) can provide self-organization, self-configuration, reduced investment, quick deployment, and simple upgrading, which are significant advantages over wired technologies. Nevertheless, IIoT devices still pose challenges in terms of standardization, reliability, security, low power consumption, and IP-based operation. Some IEEE 802.15.4 technologies have been released over latter years, such as WirelessHART, ISA 100.11a, WIA-PA, and ZigBeePRO [23], but the construction industry requires communications technologies that can operate over long distances and support equipment mobility. So, IEEE 802.15.4-based standards do not respond well to the requirements of off-road equipment used in the construction industry, as opposed to the requirements of indoor industrial facilities.

In the construction industry, some protocols exist for the transmission of monitoring data inside vehicles. However, typically, these protocols are varied and proprietary, depending on the equipment manufacturer. Wired solutions that can be found for monitoring include CAN Bus, J1939, J1708 [41], and proprietary solutions such as CAT Link and Komatsu KOMTRAX. Hence, wireless solutions like those typically used in IIoT should coexist with installed systems for a relatively long time. Because of that, the integration between wireless and wired communications poses research and technical challenges that must be addressed.

Additionally, the implementation of IIoT technologies should be connected to monitoring the performance of the machine maneuverers. Drivers and their actions can significantly impact machinery operation costs and safety. Monitoring human behavior can provide the basis for reducing machinery operation and maintenance costs and extending the life of the equipment. IIoT devices can be combined with machinery internal monitoring to include information provided by human-machine interaction. Visual interfaces should show machine status in industrial monitoring and notify operators of any operational or safety risks. Naturally, data from human-machine interaction must be kept private [42].

B. WIRELESS COMMUNICATION TECHNOLOGIES AND SERVICES

IIoT in the construction industry requires communication protocols that support dynamic, efficient, and ubiquitous information aggregation and availability [43]. Additionally, IIoT devices should support protocols for final user interfaces for operational reasons. Furthermore, construction machine systems must integrate their fieldbuses with the Internet, thus providing connection functionality to the machines. This raises several challenges such as protocol interoperability (including proprietary protocols), short-range and long-range communication, privacy, and security, among other [43], [44].

Some solutions available in the market were especially designed for industrial environments, such as IEC62591 (WirelessHART) and IEC62743 (ISA100.11a). However, these standards are based on IEEE 802.15.4, which is not intended to connect a vast number of devices [45], support long-distance communication, and mobility, as is desirable in IIoT applications for the construction industry [43]. Consequently, other approaches have been used to overcome these limitations, typically resorting to some kind of IIoT gateway. Hence, for covering long-distances, technologies such as Low Power Wide Area Network (LPWAN) have been deployed in IIoT environments [46].

LPWAN [47], [48] is considered the trendsetter in wireless networking. This is because it offers good communication range, good scalability, and low energy consumption, which are key requirements in Industry 4.0. As a result, several LPWAN solutions, including Sigfox, LoRaWAN, NB-IoT, DASH7, LTE-M1, Ingenu, and Weightless, to name a few, are currently available on the market [49]. Among them, because of their general characteristics (such as low power consumption, high scalability with long radio range, and low-cost network infrastructure), LoRaWAN [50], Sigfox, and NB-IoT [51] are adequate for most machine-to-machine (M2M) connectivity scenarios in IIoT for the construction industry.

Cellular technologies such as 5G should be considered. 5G is especially suited for three application scenarios, namely Ultra-Reliable and Low-Latency Communications (URLLC), massive Machine Type Communication (mMTC), and enhanced Mobile Broadband (eMBB). In our case, mMTC could offer a high density of connected devices, long-range, and low power consumption. Additionally, 5G can

support high data rates with eMBB, and highly reliable and low latency communications using URLLC for critical IoT and Industrial Automation. However, LPWAN support in cellular networks results in significant investment [52] as these networks operate in licensed bands. Additionally, most service provider deployments mainly target eMBB, neglecting the commercial deployment of URLLC and mMTC solutions.

Regarding non-cellular LPWAN technologies, which operate in unlicensed bands, they are expected to complement cellular technologies like 5G, contributing to services and applications. Furthermore, the integration between unlicensed bands-based LPWANs and 5G creates several opportunities, as hybrid networks can reduce the operation and implementation costs, but require more work on integration and security mechanisms. Finally, there are significant problems in using 5G in far-off construction sites, as in many cases there is limited or nonexistent 5G coverage, thus preventing the use of cellular networks for direct communication between machinery and the Internet [52].

C. MANAGEMENT MODEL REQUIREMENTS

Integrating deployed industrial monitoring infrastructures with IoT poses several challenges due to the fundamental differences between the approaches traditionally used in these environments. The former is typically wired and centralized. In contrast, the latter uses a wireless, decentralized, Internet-based approach. Given the above, construction industry management models should allow the interaction with the IIoT devices deployed in machinery, allow for more automated decisions, be less human-dependent, and not be an obstacle to intelligent systems management. Specifically, construction industry management models should meet the following requirements.

- They should be able to support the monitoring of heavy-duty machines, to detect and diagnose equipment failures. In addition, management models should allow the collection of network data coming from wireless and wired environments. Industrial scenarios generally use wired networks for fault notification and control inside their systems, and the management models should support this as well.
- They should be able to predict errors or degradations of integrated components using intelligent data analysis. Thus, techniques like micro-intelligence, edge-computing, or federated learning on IIoT components will help recognize future failures and take autonomous actions to prevent industrial losses. Furthermore, these learning mechanisms should be able to predict whether the status of the machinery is as expected or abnormal. Unlike IoT devices with micro intelligence, learning systems and forecasting can be implemented in upper layers. A more robust mechanism using combinations of neural networks and metaheuristic grasshopper algorithm GOAMLP [53] can learn to predict errors in different stages and different network elements, including machinery. The machinery operators may have no access to the status. However, a trained neural network can check the status of machines and trigger a ''power outage'' to stop them in case of imminent danger.
- Communication networks to support the operation of management systems may include long-range wireless communication, like LoRaWAN, operating in limited frequency bands (such as ISM 868Mhz in Europe). Furthermore, it might be possible to dynamically change parameters that maximize resource usage and optimize frame structure. In addition, they should contribute to the battery lifetime preservation of constrained devices through the intelligent configuration of awake and sleep periods. Finally, the configuration of IIoT device parameters may have security and safety implications. Therefore, management systems must use adequate security while managing the changes that affect machinery operations.
- Construction industry generally has high-reliability re- requirements. So the management system should constantly monitor the IIoT system performance to detect any degradation and act as soon as possible. Connection loss, packet dropping, low network utilization, and weak network response in IoT communication can affect the overall system. Therefore, management models must seek to optimize the network operation and support the integration between legacy sub-systems and new IIoT-based systems.
- In addition to managing IIoT components and industrial wired/wireless networks, construction industry management systems should also deal with machine operators information. Operators often directly impact the degradation of industrial systems, and the management models must monitor this. Integrating human and behavioral data in IIoT systems will help to improve and optimize processes. All these data should be visualized and analyzed as part of the architecture, always considering the operators' privacy.
- Finally, distributed management must ensure end-to-end security of the information in the integrated system. Therefore, this includes security at the levels of wireless communication, integration framework, and analysis/visualization platforms. In addition, management models should ensure that IIoT devices do not increase vulnerabilities in the fieldbuses of industrial systems. Hence the system must contemplate the trust management of the various devices and subsystems. Technologies such as blockchain can tackle IIoT security aspects, including secure distributed storage, non-tamper proof of the collected data from the machinery, network data authenticity, and prevention of malicious field bus interference [54].

IV. PROPOSED SOLUTION

The previous section presented requirements for the construction industry in what concerns IIoT. The current section

presents the proposed solution, designed to address these requirements.

The project intends to propose, develop, and assess an innovative technological solution for the real-time monitoring of construction industry machines, including their operational conditions, as well as the behavior of the maneuverers of those machines, as key active elements of the system. Furthermore, this project builds on a variety of data acquired from machine operators (e.g., work hours, movement parameters, operator identification), from the environment (e.g., temperature, background noise), and from the industrial machines (e.g., fuel consumption, oil and engine temperature, localization), using a machinery monitoring unit (from now on called IIoT node) or other external sources. IIoT nodes interact with Electronic Control Units (ECUs) on the monitored machines or directly acquire data from available analog sensors. The proposed framework is shown in Figure 1. The framework comprises the perception layer that establishes the connection between machines and IIoT devices. Furthermore, it includes the communication layer with gateways and cloud services and the application layer established between the integrators and the different end-user applications.

The proposal was validated through prototyping and trials in a real-world industrial scenario. The prototypes served as a tool to gather information that was later used to study, propose, and refine integrated management models in industrial environments. They will also be used for studying and developing new functionality and/or management models. The trials were deployed at Conduril - Engenharia, S.A, a Portuguese company with 62 years of experience in Civil Engineering. Conduril has hundreds of pieces of equipment and machinery, to develop engineering projects nationally and internationally.

In this context, effective monitoring of the operations, maneuverers, and vehicle status can reduce costs, prevent faults, and enhance construction process visualization. With the collaboration of Conduril, the researchers involved in this project developed a prototype for real-time monitoring of on-site processes. In addition, a variety of machines also leads to heterogeneity of motors. For example, Conduril has motors from several manufacturers, such as CAT, Cummings, Daewoo, Deutz, Iveco, John Deer, Komatsu, Perkins, Scania, and Volvo. Furthermore, Conduril machinery uses various vehicle control technologies. For instance, some machine components must be monitored through ECUs, while others are analogically monitored. Moreover, the ECUs communi- cation protocol can be proprietary (e.g., Caterpillar Direct Link (CDL)) or open (i.e., J1939). Finally, CAN bus access plugs depend on the machinery, having 8, 9, 12, or 14-pin connectors.

The following sub-sections detail the components of the construction machinery monitoring framework presented in Figure 1.

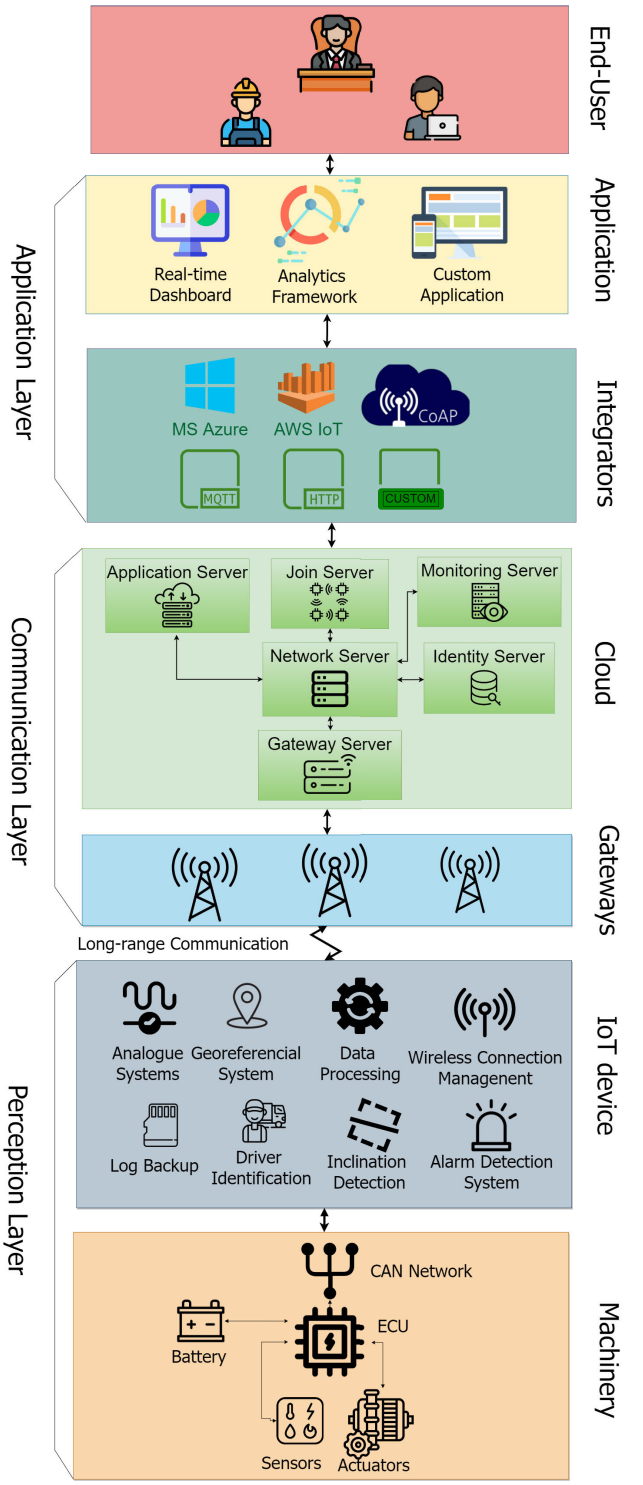


FIGURE 1. Proposed framework.

A. MACHINERY

Construction machinery is equipped with sensors, actuators, and power supply systems to control the internal components of the vehicles. These components are connected to an ECU responsible for receiving information from the sensors and sending information to the actuators. This communication

TABLE 2. Used J1939 signals (based on the requirements).

PGN	SPN	Name	Bytes	Position	Unit	Range	Resolution	Frequency
65276	96	Fuel Level	1	2	%	0 to 100	0.4% / bit	1 sec
65262	175	Oil Temperature	2	3-4	deg C	-273 to 1735	0.03125 deg C/bit	1 sec
65188	1136	Engine ECU Temperature	2	3-4	deg C	-273 to 1735	0.03125 deg C/bit	1 sec
65262	110	Engine Coolant Temperature	1	1	deg C	-40 to 210	1 deg C/bit	1 sec
65268	241	Tire Pressure	1	2	bar	0 to 10	0.1 bar / bit	10 sec
65263	100	Engine Oil Pressure	1	4	bar	0 to 10	0.1 bar / bit	0.5 sec
64929	3484	Aftertreatment 1 Fuel Control 1	0.25	7.3	state	0 to 1	N/A	0.5 sec
65271	168	Battery Potential / Power Input 1	2	5-6	V	0 to 3212.75	0.05 V / bit	1 sec
65271	114	Net Battery Current	1	1	A	-125 to 125	1 A / bit	1 sec

is standardized for most vehicles and is executed through a CAN network for the physical layer and J1939 information for higher layers.

CAN is the protocol that allows a two-wire bus to support ECUs communication in heavy trucks and off-road machines. These wires run through the entire truck structure, and the ECUs must be connected to them to communicate using J1939 messages. In addition, monitoring tools to evaluate machine performance must access the communication bus through J1939-compliant plugs. These connectors are designed to allow CAN_H, CAN_L, power, ground, and extra functionalities defined by each manufacturer. The interface is usually accessible in heavy-duty vehicles and has a female connector to read J1939 messages.

Nevertheless, not all manufacturers implement the J1939 standard connector or follow the same pinout. For example, Caterpillar defined its own pinout to transmit J1939 information, including pins to send Caterpillar Direct Link (CDL) bus information. In addition, we can find brands, such as Volvo, that make the CAN bus available through 16-pin ODB connectors, or Komatsu that uses a 26-pin connector to plug monitoring tools. This diversity of connectors has proved challenging in implementing our monitoring prototype in the field, requiring considerable effort to determine the specificity of each solution, in order to gain access to CAN_H and CAN_L channels. As expected, industrial solutions do not always follow predefined standards and often develop their own proprietary solutions to explore competitive advantages.

Moreover, CAT has defined its own CAN_H and CAN_L lines to collect J1939 data. When a monitoring tool is connected to the CAN bus, J1939 data is expected to be available at the standardized frequency when sniffing the bus. Nevertheless, CAT does not make all J1939 information available on the bus. Instead, it uses the proprietary CDL protocol, for which no information is available online. To overcome this, several forums suggest implementing external monitoring solutions in CAT and purchasing CDL translators or mediators that allow having J1939 data available.

For standardized machinery, J1939 is framed in the CAN physical layer [41] for communication with ECUs. The J1939 upper-layer protocol [41] is used by heavy-duty vehicles and machinery to send and receive information from ECUs. The Society of Automotive Engineers (SAE) released J1939 to communicate critical vehicle information in a standardized manner. The messages transmitted using J1939 include oil temperature, coolant temperature, oil pressure, battery potential, and many more [41]. A tool to monitor truck/machine behavior must understand the messages sent over the CAN bus and encapsulated in J1939. SAE has defined a list of PGNs (Parameter Group Numbers) containing one or more critical signals in the CAN message payload. These signals are called Suspect Parameter Numbers (SPN) and establish the name of the signal, the number of bytes, position, unit, range, resolution, and frequency. Based on the Conduril company requirements, Table 2 shows the J1939 signals that the prototype contemplates. The PGN is an 18-bit number found in the identifier of a CAN message. Moreover, PGN is placed between the three priority bits and the eight source address bits, totaling the 29 bits of a CAN 2.0B extended frame. Each message has a data payload of 8 bytes, where one or several information signals can be carried. SAE defined 1 byte for signal values that require low resolution and 2 or 4 bytes for those parameters whose wide range and precision are necessary. Finally, 4 bits are used for control messages.

This information was extracted from various portals and is available online. Since the standard where SAE defines these values is plain text and difficult to understand, several applications can load a PGN/SPN database and automatically interpret J1939 frame traces. This is the case of Vector's CANdb++ software.

B. IoT DEVICES

The devices, or IIoT nodes, are the essential elements of the architecture, and are represented in Figure 2. IIoT devices allow interaction with heavy machinery, providing access to working parameters, and machinery behavior data, through a wide area network. These devices comprise hardware components and software algorithms to fulfill monitoring, management, communication, intelligence, and security between the industrial and network infrastructures. The main hardware modules are:

- **Pycom Module:** This is based on LoPy4, a development board that supports Bluetooth, Wifi, SigFox, and LoRa. LoPy4 uses the ESP32 Espressif chipset and enables to program and connect different IoT solutions. It uses a dual-core 32-bit Lx6 microprocessor with

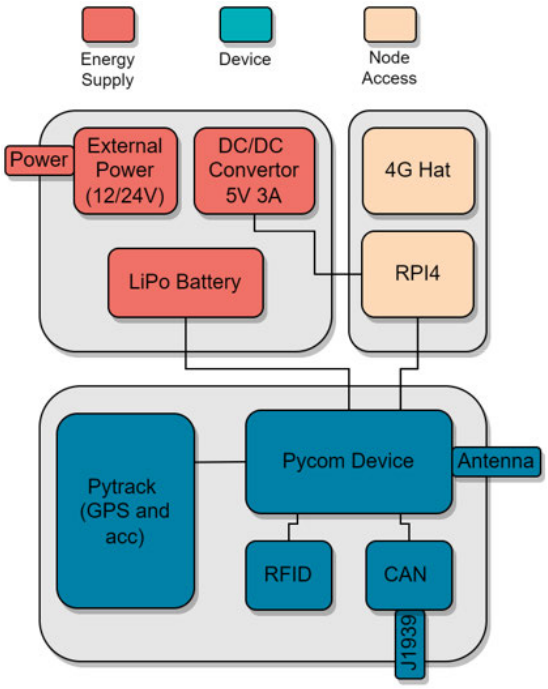


FIGURE 2. IIoT nodes block diagram.

hardware floating-point and Python multi-threading. Moreover, it includes a ULP coprocessor to monitor General-purpose input/output (GPIOs), Analog-to-Digital Converter (ADC) channels, and internal peripherals. Furthermore, it includes 520Kb+ 4Mb RAM and 8Mb external flash memory. It supports Micropython, which enables programmers to take ad- vantage of the functionality of a high-level language. Pycom devices were chosen for this solution because of their features that fit the needs of the solution. It supports several protocols, including LoRaWAN and Wifi. In addition, it allows communication with CAN networks to analyze the frames coming from the machinery. Finally, this device has a series of libraries and codes that ease the implementation of the solution, which other devices, such as Arduino, Texas Instruments, or others, do not offer.

- **Pycom Pytrack:** Pycom designed this shield to add sensors and features to microcontrollers. For example, Pytrack provides accurate GPS functions, since it can connect to Glonnas, Galileo, and QZSS for location services. Besides, it has a 3-axis accelerometer that can provide speed, acceleration, roll, and pitch. Pytrack grants MicroSD card compatibility, battery charger, and safe boot support.
- **CAN Transceiver:** This element transforms the differential signal of the CAN Bus into logic outputs and vice versa. This transceiver is built with TCAN330x family chips, allowing accepting speeds up to 5 Mbps. In addition, TCAN330x has a silent mode that enables the node to sniff the CAN bus passively.
- **RFID** An RC522-based reader was selected because this is a widely supported component. The module reads the drivers' information via one of the SPI interfaces available on the node.

The main software functions that the devices accomplish are:

- **Read GPS:** This module was implemented through L76GNSV4, MicroPython library, to obtain L76 Global Navigation Satellite System (GLNSS) information, thus enabling the use of the GPS functions in Pytrack. In addition, through this module, it is possible to obtain longitude and latitude and to update the module's internal time.
- **Read CAN Information:** This module was implemented using a callback function. CAN messages received from the transceiver trigger the callback function and are stored in a dequeue (a Python class). Moreover, the function filters the messages based on their PGNs, updating a dictionary with the more recent information from J1939 signals.
- **Interpret J1939 data:** This module takes the filtered data in the callback function and operates on it. The data stored in the dictionaries was saved with their respective PGNs and payload. This function maps a PGN with the corresponding value in the payload, extracts it, multiplies it by the resolution, and adds the offset.
- **Read RFID Information:** This is a 5-second timer used for periodically reading information from the RC522 module.
- **Packet Format:** Once the external information has been read, extracted, and interpreted, this module compiles the information and sends it via LoRa using the established format.
- **Save and Read SD card data:** The data sent via LoRa plus the values saved in the dequeue are stored as backup on the SD Card. At the same time, the values of the dequeue are transformed using a format that can be analyzed by monitoring applications.
- **Save and Receive LoRaWAN data:** Before sending and receiving information, the node must be activated within the network. Hence, information is exchanged with the gateway and servers to activate the module. Furthermore, the working frequency, spreading factor, data rate, and additional functionality must be set.
- **LoRaWAN Activation Key Management:** The Over-The-Air (OTA) activation method was chosen due to security. OTA is the most reliable activation method since activation keys are interchanged in each new process to keep the device safe. This module provides key management functionality for each new session.

The IoT devices used in this project use a high-level microprocessor programming language. Microprocessors use timers and interrupts to break the main code loop. These tools are used in this context to read the monitoring data coming from the machine. Figure 3 shows the general flowchart of the node operation under monitoring conditions. First, node

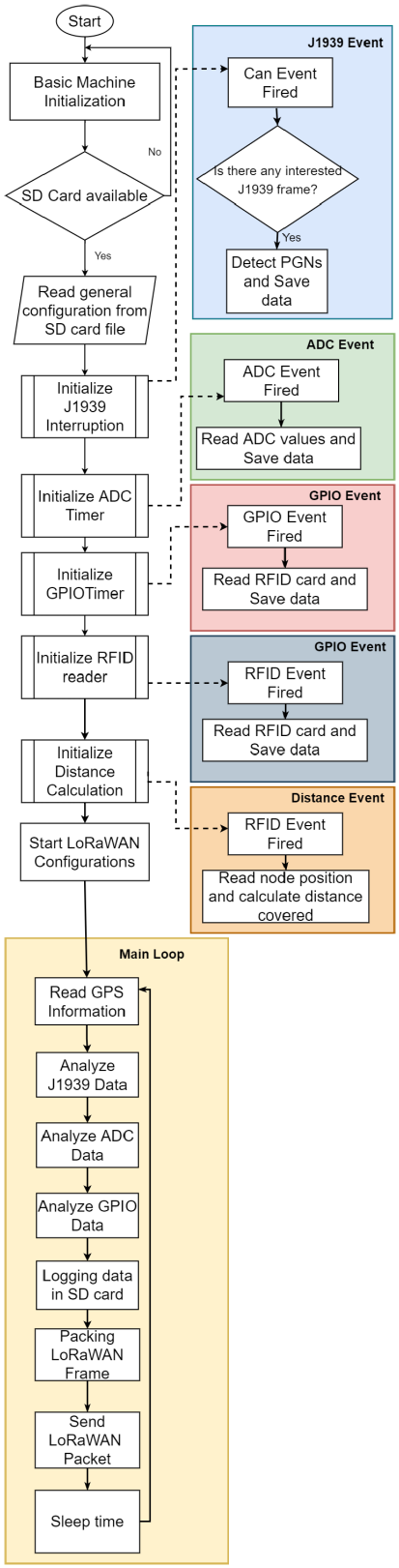


FIGURE 3. IoT device Flowchart.

configurations and operational code are placed on an SD card. These configurations allow the devices to adapt to the specific configurations of each machine, considering what type of data will be found in J1939, ADC, and GPIO. Once the node is initialized, the various modules executed by the node are activated. These include the J1939 read function, which will be activated whenever valid data is detected on the CAN bus. Once each J1939 frame is read, its data will be extracted, as well as the PGNs, and saved to be analyzed in the main loop. The ADC and GPIO reading routines correspond to functions that will perform readings on the status of ADC and GPIO features. For ADC, it allows reading of the sensors that are part of the connection with the ECU and must be read analogically and transformed into digital values. In contrast, the GPIO allows reading the states of the alarms generated by elements inside the machinery. Furthermore, the code contains a function for RFID readings, allowing the analysis of the driver's data every time he/she places the ID card near the device. Finally, the distance covered by the machine is calculated. Within the main loop, periodic position readings are performed, and the data is prepared to be packaged and sent by LoRaWAN. In addition, all data from each routine is saved as a log backup on the SD card. The backup data allows further offline analysis of the collected data.

C. GATEWAYS

The gateway is the network element that enables communication between a device and the LNS (LoRaWAN Network Server) [55]. In the implementation, a LoPy4 was used because Pycom and its firmware allow dual node-gateway implementation. Considering this, LoPy 4 was programmed with the available libraries, modifying them as needed for compatibility with our environment. Therefore, we configured the ISM 868 MHz frequency band, the spreading factor, the NTP server, the Wifi credentials, the server's name for the management platform, and the respective port.

A private gateway was configured by programming the pycom. The advantages of having a private gateway may include higher airtime capacity of LoRaWAN frames, a higher number of bytes per frame, greater control of network elements, and effective positioning management of the gateway in construction zones. However, this does not preclude the need for a stable Internet connection, to communicate with cloud servers.

D. CLOUD

The proposed solution requires cloud services to receive and manage the information. It also requires elements to manage the used gateways, applications, devices, and users. Furthermore, it was established as part of the requirements for implementing long-range communication. Therefore, LoRaWAN has been chosen and used within this approach, since it meets the requirements regarding low-power and long-range communication for IoT. LoRaWAN is an open networking standard that offers secure bi-directional communication, mobility, and management services that fit industrial implementations like this one. TheThingsNetwork (TTN) Stack community services were used to implement LoRaWAN services.

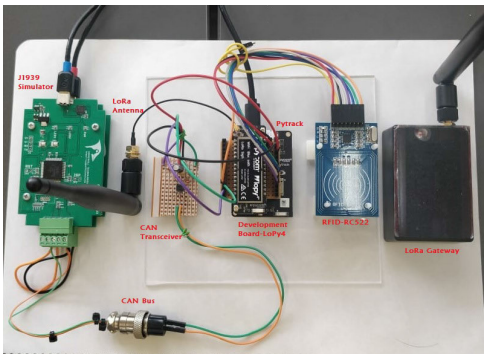


FIGURE 4. Emulation testbed.

TTN is a collaborative ecosystem released by Things Industries to develop and deploy networks, devices, documentation, and solutions over LoRaWAN. IoT devices establish LoRa communication with public gateways made available by the TTN services. In addition, the TTN platform allows us to implement the necessary servers to establish, manage and communicate with the devices and gateways. This platform was installed on cloud machines belonging to our research group.

Within the TTN stack, servers were enabled to manage network elements such as IoT devices or gateways, security, and user access. For example, the gateway server receives the information in LoRa format from the devices and forwards it to the network server. The network server is the most critical element of this layer since it manages all the information and monitors the network parameters to establish point-to-point communication in the infrastructure. In addition, it manages the security elements used in the activation processes of the devices and users. Finally, application servers redirect the formatted information (in javascript format, for example) to the integrators so that external applications and dashboards can consume it. In addition, there are methods for securely activating devices, checking the identity of messages, and monitoring network elements. All these tools make the TTN platform a powerful tool for implementing LoRaWAN communication in industrial IoT approaches.

E. INTEGRATORS

Integrators connect the information stored in the cloud to third-party applications, data analyzers, or dashboards. Within the TTN platform, several integrators are defined with various purposes; however, this project implements MQTT integrators. In addition to serving as a telemetry protocol, the MQTT protocol supports network management tasks in the infrastructure, which will benefit the following stages of the integrated management model.

First, the TTN platform's plugin provides MQTT broker functionality for different purposes, including managing LoRaWAN devices. Two methods are accepted for clients of this broker: Subscribing to Upstream Traffic and Publishing Downlink Traffic. Second, from the application perspective, an MQTT connector service allows users to subscribe to the topics defined in the broker using the MQTT connector. This connector defines how the information will be extracted from a decoded payload and how the LoRa Gateway scans the file. Finally, this connector automatically creates devices in TheThingsBoard, since it has a parameter to identify new devices and create them directly in the dashboard.

F. APPLICATION AND DASHBOARD

It is necessary to implement a dashboard and third-party applications to analyze the data coming from the monitoring of the machinery. For this project, two main applications were used for data analysis and data management of the machinery and their operators. The first one provides a dashboard using the tools available in Things-board, through which processes, data, alarms, and historical data obtained from the machine are monitored in real-time. Furthermore, this dashboard configures the necessary gadgets to implement a detailed view for operators or managers. In addition to the dashboard, a web application was developed to manage the machinery's comprehensive work information, such as traveled distance, operating driver, and type and amount of work done. Furthermore, this management platform can automatically produce a detailed worksheet, thus precluding the need for manual reporting. The management application was implemented through radzen, which eases the creation of.NET Core web applications.

V. TRIALS AND EVALUATION

To assess the proposed solution, we implemented and deployed a prototype in two real-world trials at Conduril's facilities at Sines and Ermesinde. Nevertheless, we developed an emulator before implementing the prototype and used it for some preliminary tests. The following subsections describe the emulator, the prototype, and the field trials.

A. PRELIMINARY TESTS USING AN EMULATOR

The emulator was built to perform several preliminary tests before moving to a prototype implementation and field trials. The emulator is represented in Figure 4 and comprises a J1939 simulator, IIoT device (with antenna, CAN transceiver, Pytrack plus LoPy4, and RFID reader), and LoRaWAN gateway. The J1939 simulator allows entry of the PGNs, data, transmission method, and message frequency between two development boards that support CAN communication. The emulator also includes Copper- hill's JCOM1939 software, which can simulate two ECUs complete with address, industry number, vehicle number, function, manufacturer code, and instances. Additionally (not represented in Figure 4), we implemented the network infrastructure, TTN platform, LoRa gateway, and a simplified dashboard. Using this emulator, we defined and performed six types of tests described below in this preliminary experimental phase.

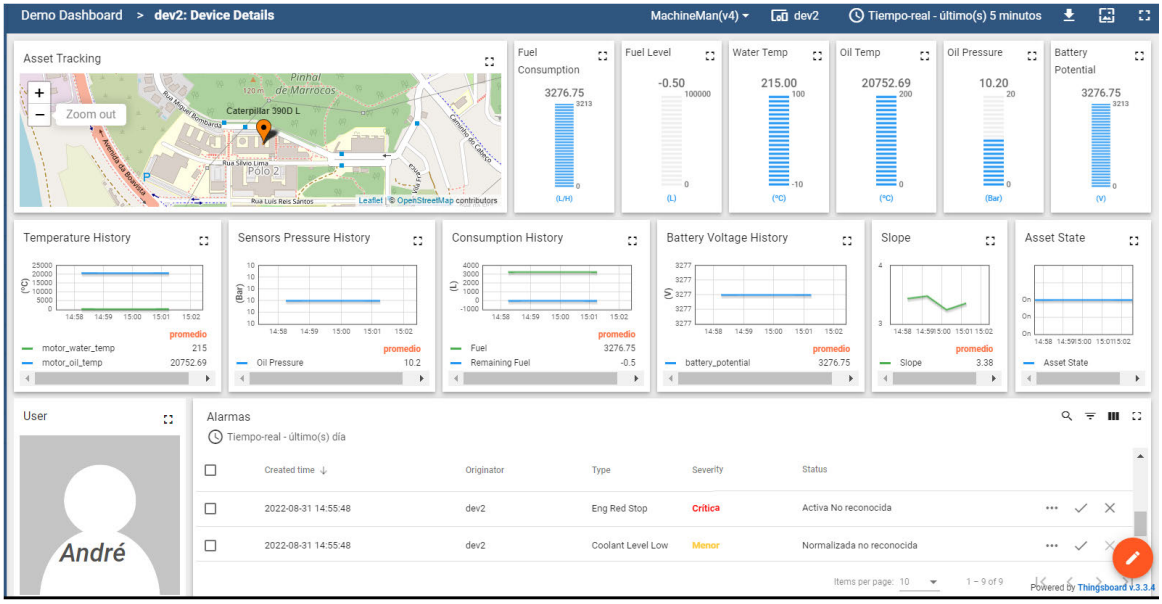


FIGURE 5. Real-time information dashboard.

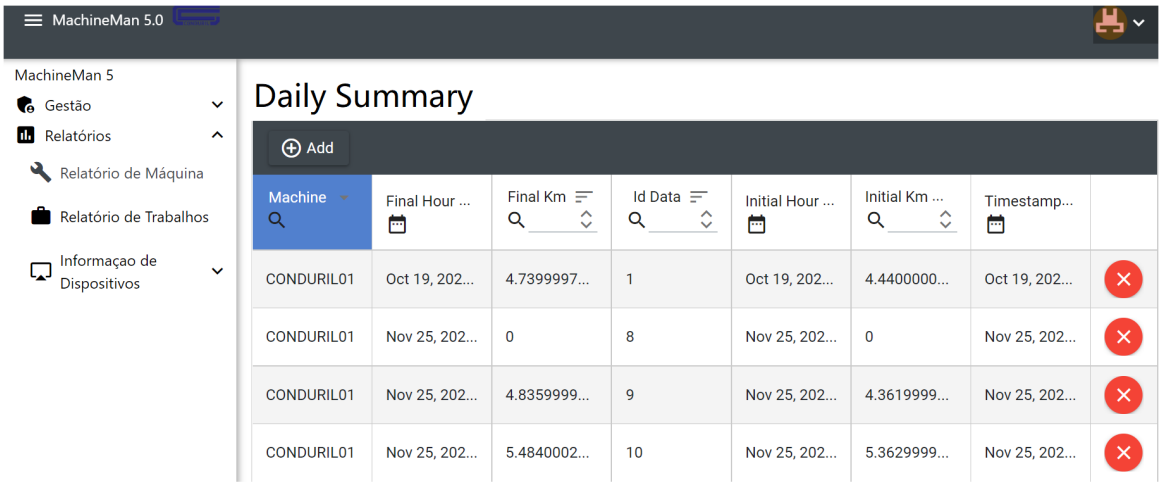


FIGURE 6. Management platform: Daily summary.

1) NETWORK INFRASTRUCTURE AND DASHBOARD TESTING

Random value generation was used to experiment with the devices within the LoRaWAN network and test the dashboard. Pseudo-random functions generated the J1939 values, with the sole purpose of checking the devices' operation and connection capabilities. These tests allowed debugging of the TTN platform, the MQTT connection, the LoRa gateway, and the dashboard. Communication was performed in this controlled setting to verify the correct operation of each element.

This experiment targeted two main modules. The first one was the Dashboard that shows the information generated and collected through the IoT devices in real-time. Figure 5 shows the implemented Dashboard where the GPS position information, fuel consumption, engine water temperature, engine oil temperature and pressure, and battery voltage can be seen. In addition, the history of each of these parameters is shown for analysis. RFID card identification and alarms generated in the system are also included.

The second module provides management functionality of construction site elements based on information from IoT devices. This module automatically collects and associates the information with site elements such as machinery, devices, and work. The module allows the management of all the machines in the company's inventory, in this case, Conduril S.A. Furthermore, it details the work performed, the employee who performed it, the time, and the activities. Finally, we have access to the summarized information of a day's work by machine, as shown in Figure 6. This comprises GPS information, identification, and machine data such as

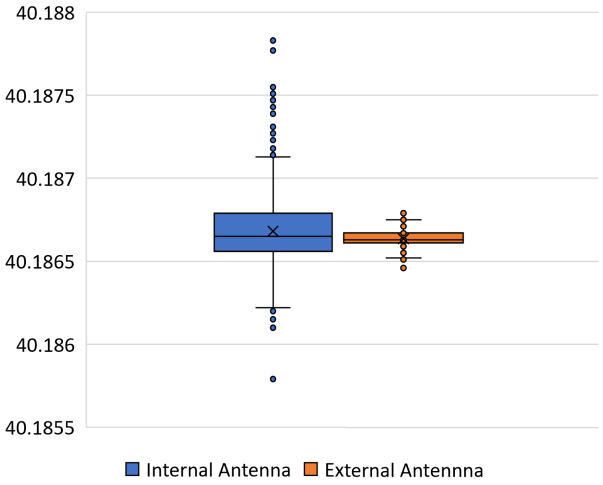


FIGURE 7. Latitude measurements using internal and external antennas.

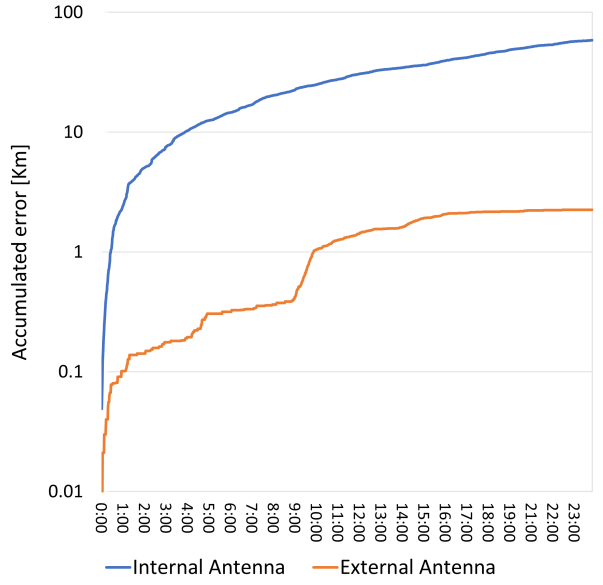


FIGURE 8. Daily accumulated error in calculating the travelled distance with internal vs. external antenna, while the node is at rest.

initial and final kilometers, initial time, final time, and work identifiers.

2) COMMUNICATION RANGE TESTS

LoRa radio allows long-distance communications, and this is, in fact, one of the features that have led to the choice of this technology. In the initial test scenario, the distance between the device and the gateway was less than 10m; therefore, a long-distance test was required. The test was conducted in the vicinity of Coimbra city, with distances of less than 1km, 1km, and 1.5 km. The tests were successful, obtaining almost complete connection for these distances with low packet losses. These tests were executed using a spreading factor (SF) of 7.

TABLE 3. Distance calculated by the IoT prototype compared to the distance calculated using commercial GPS devices such as smartwatches and smartphone.

Distance [Km]	Route 1	Route 2	Route 3
IoT device	**3.045**	**2.745**	**0.98**
Smartphone	3.02	2.75	1.06
Smartwatch	2.82	2.8	1.02

3) GPS TEST

This test allowed us to understand better the Pytrack shield's limitations in communicating with the GPS satellites. Experiments were performed on de-powering the board, de-powering during short times, de-powering during long times, and changing initialization parameters. The tests were performed daily in the same place, in the same position, and avoiding obstructing the GPS antenna. In addition, tests showed that implementing the Hot Start method at GPS initialization can reduce the GPS fix time after a prolonged disconnection, since Hot Start remembers the last valid position before a module restart.

Once the operation dynamics of the coordinates data acquisition libraries were understood, tests were run to optimize data acquisition under adverse conditions. The first of these tests was to analyze the coordinate acquisition conditions when the node was stationary, since construction machinery spend long periods in the same area, and the accuracy of the location would allow a better understanding of the risks within the construction site. Next, we compared the impact on data accuracy when using the integrated antennas in the pytrack shield and external active antennas. Figure 7 compares collecting latitude data using an internal antenna versus an external one when the node is at rest in the same position. The figure shows that the latitude obtained without an external antenna is considerably less precise and less accurate. Using an internal antenna, data collection variability is relatively high, with a standard deviation of 0.00016567. On the other hand, data collected with an external antenna leads to much higher precision, with a standard deviation 0.000064774, which represents an improvement of 64% in relation to the previous case. A similar behavior was registered in the case of longitude measurements.

Longitude and latitude measurements variability leads to error in the estimation of the travelled distance. Figure 8 shows the distance calculated with the data obtained without an external antenna and with an external antenna, for a stationary machine. Note that if the machine is stationary the calculated distance should be zero. Nevertheless, with an internal antenna, the accumulated distance error was more than 60 km in one day of testing with the prototype. On the other hand, with an external antenna, the calculated distance reaches approximately 2.4 km. These values indicate that calculating the distance using an external antenna led to an increase of 96.47% in performance.

Although precision and accuracy highly benefit from using an external antenna, the effects on the energy

expenditure with this antenna should be analyzed. External antennas can consume between 3 to 20 mA, so their impact is non-negligible for those scenarios where power consumption is a concern. Fortunately, in the case of the scenarios at hand, the devices will be constantly connected to the vehicle's battery, which means that the use of external active antennas will not pose any problems.

As mentioned above, travel distance information is used in several management reports. Therefore, it is necessary to determine the accuracy of different devices when in motion. For this purpose, three routes of 3km, 2.8 Km, and 1Km were established, as these distances were deemed reasonable in specific construction fields. Moreover, three different types of devices were used: an IoT device, a cell phone, and a smartwatch. Inside each node, several processes were executed simultaneously, performing J1939, ADC, and GPIO readings. Table 3 shows the various devices' results for the considered routes. As can be seen, the distances calculated by each node are similar.

4) RFID TESTS

The objective was to verify the operation of the RFID- RC522 module under a variety of conditions. Several RFID cards were successfully tested. This test allowed us to identify a misconfiguration of the RST pin reader that affected the module's reset state, preventing it from operating correctly.

5) CAN-J1939 TEST

The objective of this test was to check the operation of the simulators, CAN bus, and transceiver. The experiment was performed by modifying the number of frames sent by the simulators, and the frames frequency. In addition, the test scenario was subject to forced restarts, seeking to understand if they caused failures within the CAN bus in a real environment.

During the tests, we tried to understand the behavior of the IoT device under increased load on the J1939 interrupt. The process the device executed was the one depicted in 3. Inside the microprocessor are the processes and functions of the main loop; simultaneously, the different asynchronous events must be processed. Pycom devices handle these events and interruptions sequentially, placing the calls and their variables in a queue until they are processed. Furthermore, this queue has limited memory, so it is possible that the processor cannot handle the interrupt and does not generate the corresponding output. Except for the CAN call with the J1939 frames, the rest of the events are fired by timers, so we chose to modify the number of J1939 frames sent by the simulators and evaluate the node's behavior.

Within the J1939 simulator, we varied the number of frames from 50 to 1500, executed a representative number of times for each frame rate, and analyzed the processing time and the number of times the callback functions were activated. The data were analyzed per cycle. Each cycle was considered separately, since the module goes to sleep after sending each LoRaWAN packet. The following graphs refer

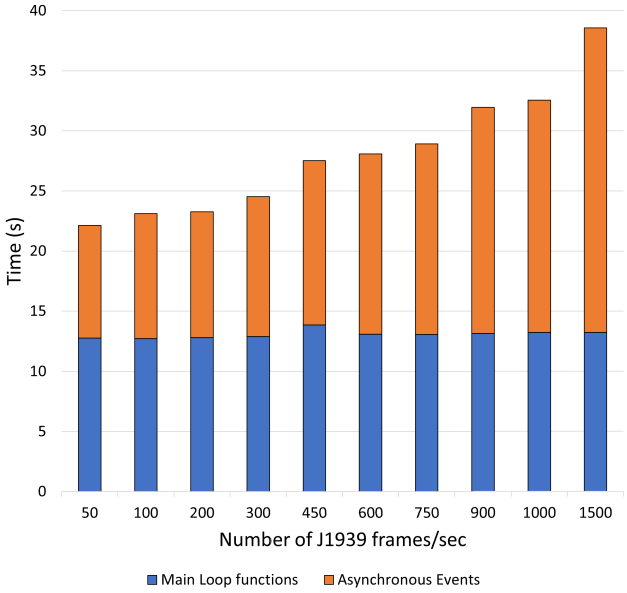


FIGURE 9. CPU processing time for Main Loop Functions and Asynchronous Events.

to data obtained within one cycle, since all variables were deleted at the end of the cycle. In addition, the resolution times of the main loop functions were measured to compare them with the times obtained in the resolution of the interrupts. Figure 9 shows the cumulative processing time of the node for the main loop functions and the interrupt functions. The main loop functions were optimized so that the operations of data analysis, writing to the SD card, and packaging were significantly not affected by the load imposed by the interrupts.On the other hand, the cumulative processing time of the interrupt functions increases as the call load of the J1939 frame functions rises. Within the main loop, sleep time is considered to control the sending of LoRaWAN frames to the gateway. Considering this time of 60000 ms plus the processing time of the main loop functions, the processor uses most of this time to respond to interrupt calls. With a minimum sending of 50 J1939 frames, almost 10,000 ms can be used to handle the interrupts. However, even though the number of frames per second increases to 1500, the time does not go beyond 25000 ms. The processing utilization time is essential, as it directly affects the microcontroller's ability to handle the generated interrupts. Therefore, as the processing time increases, the probability of not responding effectively to interrupts increases. As several modules involve alarms and interrupts, it is crucial to keep the processing time as close to optimal as possible to maximize the time available for responding to interrupt calls.

To analyze which interrupts require more processor time, the cumulative time to handle each interrupt per duty cycle was measured. The interrupt functions were optimized to be the least time-consuming. Table 4 presents the cumulative times per cycle for the five asynchronous events of the node. As expected, the time to handle J939 frame calls increases as the number of sent frames increases. However, even though

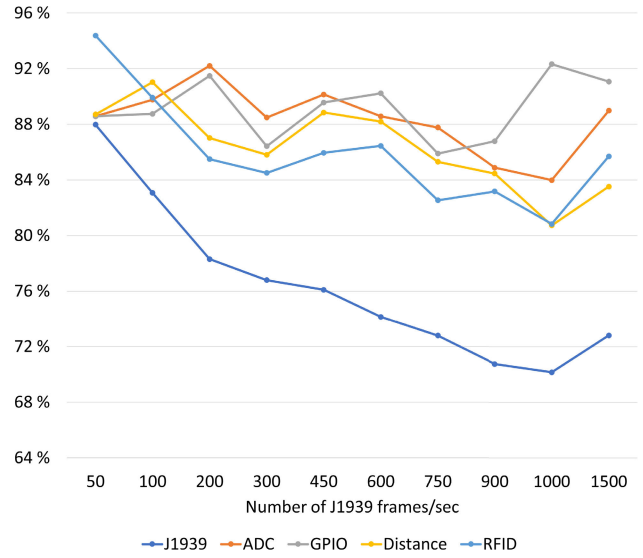


FIGURE 10. Percentage of handled Asynchronous Events vs Expected.

the number of sent frames is high, the response time is fast enough not to increase the accumulated time considerably.

Comparatively, the response time of the ADC and GPIO read functions is low, indicating that the functions and libraries for those cases respond quickly to the calls. However, on average, the distance and RFID read functions take considerable time to respond, with a high standard deviation. In the specific case of RFID readings, their values are pretty high and are similar to the processing time of J1939 calls when receiving 600 frames per second. This suggests that a way to optimize driver identification readings should be sought.

As mentioned, the callback functions' processing time can directly impact the ability to handle the various interrupts. Figure 10 shows the percentage of resolved interrupts vs. expected interrupts. The number of resolved callbacks was counted, and the number of calls that should have been resolved was calculated as a function of the total cycle time. The J1939 interrupts are the most affected, showing a clear downward trend as the number of frames sent per second increases. At a low number of frames per second, a resolution of almost 90% can be obtained, decreasing to almost 70% when the number of frames sent per second increases. This means that when the number of frames is high, there can be 30% of frames that need to be analyzed and saved for further analysis. These scenarios should be analyzed on real machines to determine the impact of frame losses on the actual monitoring. Concerning the ADC, GPIO, Distance, and RFID interruptions, we can observe a downward trend in the percentage of handled callbacks, but without reaching values below 80%, which is within typical values and considered expected for these scenarios [14], [56], [57].

6) LONG RUN TESTS

These tests allowed the test scenario and the subsequent prototype to be subject to long sessions of the previously

FIGURE 11. Prototype inside view.

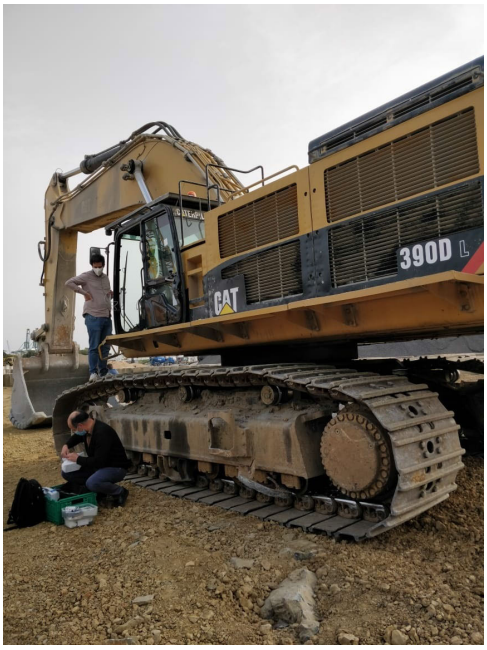


FIGURE 12. Installing the prototype in a real-world construction machine.

described tests. Thus, the network infrastructure, the GPS, the RFID, the simulators, and the J1939 communication were tested together over several days. These tests allowed us to understand how the prototype reacted to the stress of several days running as if it were connected to the machines. In addition, these tests were centered on discovering if the device got stuck after continuous operation over long periods of time. The device behaved as expected, even after several consecutive days of uninterrupted operation.

B. PROTOTYPE

The subsequent step was to develop a fully operational prototype for deployment in real, heavy-duty construction machinery. The block diagram of the implemented solution prototype is presented in Figure 2. As programming and debugging the module in industrial scenarios can be challenging, a Raspberry Pi 4 (RPI 4) with a 4G hat was included to allow external communication with the module. In addition, the

TABLE 4. Processing mean and standard deviation times, in ms, for the various types of asynchronous events.

	J1939		*ADC*		*GPIO*		*Distance*		*RFID*	
frames/sec	**Mean**	**Std**	Mean	Std	Mean	Std	Mean	Std	Mean	Std
50	**711.02**	**61.94**	74.52	4.90	54.12	3.62	1,353.82	456.91	7,101.96	604.91
100	**1,269.93**	**74.94**	73.39	4.10	53.58	2.98	1,824.88	988.45	7,109.24	1,169.00
200	**2,438.31**	**128.06**	75.20	5.49	54.17	3.88	1,164.72	604.03	6,656.33	488.02
300	**3,426.96**	**253.99**	75.29	5.49	53.29	2.76	1,517.63	576.87	6,497.98	300.63
450	**5,508.68**	**443.92**	75.37	6.92	54.86	3.58	1,492.34	562.11	6,463.40	271.13
600	**6,848.81**	**613.26**	72.20	1.04	54.30	2.58	1,369.07	754.51	6,603.98	358.09
750	**8,182.62**	**202.45**	75.82	6.72	54.42	2.89	947.97	311.10	6,516.87	186.35
900	**10,448.92**	**527.94**	71.41	7.28	53.74	0.56	1,636.51	516.81	6,523.96	294.27
1000	**11,567.63**	**700.02**	72.94	6.04	60.13	19.96	1,292.68	515.08	6,278.58	328.83
1500	**17,055.45**	**1,121.20**	73.94	5.24	56.30	4.18	1,453.61	569.67	6,631.41	216.70

TABLE 5. Comparison of machinery's parameters information.

Machine Values	**Remaining fuel**	Ignition	**Motor Consumption**	**Motor Temperature**	**Motor water Temperature**	**Oil Pressure**	**Tire Pressure**	**Motor Oil Temperature**	**Battery Potential**	**Battery Current**
CAT d6t xl	No	Yes	No	No	No	No	Check	No	No	No
Texa Tool	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes	No
CAT 4 32	No	No	No	No	No	No	Check	No	No	No
Atlas Copco roc d7	No	Yes	Yes	No	Yes	Yes	No	Invalid	Yes	Invalid
Wirtgen w100f road mining	Fuel Used	Yes	Yes	No	Yes	Yes	Check	Yes	Yes	Invalid
New Holland	Fuel Used	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Invalid

RPI 4 allows tunneling and SSH-based connections to access the module. Also, applications like screen and ampy allow to upload/download firmware files and watch the module's behavior. Finally, a battery and a DC/DC converter were also added. Figure 11 presents a view of the implemented prototype.

C. SINES TRIAL

The next project phase was to deploy and test the implemented solution in real equipment. This was done at Conduril's site in Sines, in southern Portugal. The objective of this first trial was to install the prototype on a few machines (Fig. 12) and perform several tests to check the prototype's connectivity, installation, and operation. The installation should allow the collection of information about the ECU of the chosen machine, perform connectivity tests, monitor the prototype's operation, correct problems, and get a first dashboard view of real machine data.

The first tests were performed on the CAT excavator using the developed prototype, the monitoring tools, a Picoscope oscilloscope, and the J1939 simulators. Unfortunately, these tests were unsuccessful, as the prototype failed to obtain J1939 information from the CAN bus. Furthermore, the analysis of the data collected with the tools showed no valid J1939 data. Due to these results, it was decided to repeat the experiment on a different machine from a different manufacturer. The second machine was a New Holland tractor with a J1939 connector. After installation, the tests showed that the prototype worked properly after identifying and solving specific errors on parameters that were not being calculated correctly.

The following conclusions could be drawn from the Sines tests: the used CAT excavator does not support J1939, as CAT machinery uses other proprietary protocols to make the J1939 information available on the CAN bus; New Holland equipment supports J1939, which eases the implementation of integrated monitoring solutions.

D. ERMESINDE TRIAL

The second field trial occurred at Conduril's site in Ermesinde, north of Portugal. The trial's objective was not to test the prototype but to collect data from different machines to analyze the supported protocols. This time four machines were analyzed: two CAT machines, one Atlas Copco machine, and one Wirtgen machine. Again, monitoring tools (e.g., Texa Tool) that allow Conduril personnel to perform this activity were used as reference. Although, as expected, the CAT machines did not provide J1939 information on the CAN bus, the other machines provided J1939 data, which was collected for further analysis. Table 5 shows which parameters were available in each machine.

TABLE 6. Periodic J1939 messages extracted from Conduril's machinery data analysis.

Message	Name	Frames/sec
EEC3	Electronic Engine Controller 3	4
EEC1	Electronic Engine Controller 1	10
AT1MG	Aftertratment 1 Intermediate Gas	2
AMB	Ambient Conditions	1
HRLFC	High Resolution Fuel Consumption (Liquid)	1
SHUTDN	Shutdown	1
OHCSS	Off-Highway Engine Control Selectrion States	2
LFE	Fuel Economy (liquid)	10
EEC2	Electronic Engine Controller 2	20
ET1	Engine Temperature 1	1
IC1	Intake/Exhaust Conditions 1	2
EFL_P1	Engine Fluid Level /Pressure 1	2
AT1T1L	Aftertratment 1 SCR Reagent Tank 1 Information	1
VEP1	Vehicle Electrical Power 1	1
	Total	**58**

The devices stored the collected information inside the machines, allowing for post-monitoring analysis. In addition to the values in Table 5, the periodic messages sent on the CAN bus were evaluated. These periodic messages may or may not contain the monitored signals and are sent by LoRaWAN. In any case, they are also stored for further analysis. In addition, these messages allow the evaluation of the maximum number of frames per second (fps) generated by each machine. Table 6 summarizes the obtained values. The theoretical maximum number of CAN messages is 1500 fps. On other hand, it is considered that the maximum number of frames per second in real world scenarios is about 1300. Under optimal conditions, the analyzed machines sent only 58 periodic frames per second. Some messages are non-periodic and can increase the number of frames per second; however, they are well below the theoretical and practical maximum limits.

VI. CONCLUSION AND FUTURE WORK

Management of industrial systems, along with IIoT, can improve construction site operations, reduce maintenance costs, improve productivity, and extend the life cycle of machines. However, many industrial systems still rely on relatively old technology, which represents a considerable challenge in what concerns IIoT integration and management. In the case of the construction industry, significant investments in machinery are required, and their monitoring and management are, typically, proprietary. Additionally, these machines tend to be used for long periods of time and do not adapt efficiently to emerging technology offers.

To the best of our knowledge, this is the first paper to present a solution for the integrated management of construction industry equipment. After analyzing existing management approaches and requirements in this industry, the proposal scope, objectives, and implementation were presented. The solution seeks to be implemented in machines regardless of the brand, company, or engine. Moreover, it was subject to testing in emulated and field trials using real industry equipment, which allowed the identification of several issues and challenges.

The proposed solution enables the integrated and intelligent monitoring of construction machinery, applying it to legacy technology, current systems, and future equipment. Furthermore, integration using the proposed approach enables long-distance LP-WAN communication with the various subsystems and machines belonging to a given company, making them accessible even in low-coverage areas.

The main element of the integration solution is the IoT device, so its behavior, when subject to various J1939 frame loads, was evaluated. In addition, a study of the effect of using micropython as a high-level language in interrupt processing was performed. When pycom is subject to high J1939 frame loads, it can suffer read losses and hence packet losses of up to 30%. Nevertheless, in real-world scenarios such as those at Conduril's construction sites, frame rates are relatively low, leading to negligible losses of less than 1%.

In what concerns the machinery, some conclusions can be drawn. First, some parameters and PGNs need to be sent through J1939. Furthermore, although some machines use standardized solutions at the protocol level, they use plugs and connectors that do not conform to the standards. Second, J1939 information can be analyzed, converted, and presented through CAN bus sniffing. SAE standardizes some J1939 parameters, but not all are implemented by manufacturers. Third, information about the CDL protocol is not public; however, it is possible to use external solutions to perform CDL translation and obtain the corresponding J1939 values. Integration of IIoT devices is possible and allows monitoring of the behavior of heavy machinery if they use standardized protocols. Proprietary tools have competitive advantages but are an obstacle to managing devices in heterogeneous environments. Finally, there is a risk of junk communication failures on the part of the node and the transceiver, although the chances are low if the node is in silent mode, as it blocks any communication from the node to the CAN bus.

The presented work is a first step towards the integrated management of construction industry machinery and systems. As a result of this work, many topics for future work have been identified. The ones that will be addressed shortly include an analysis of wired and wireless technologies that better fit the industrial scenario. Additionally, the refinement and enhancement of the proposed model and implementation will be pursued, as well as the development and

testing of intelligent management applications for the construction industry. Moreover, approaches for predicting abnormal machinery status will be investigated, along with solutions for including micro-intelligence in IIoT devices. Further- more, future stages will evaluate the combination of neural-network-based approaches with metaheuristic algorithms like GOAMLP. Finally, the implications of combining the FCAPS network management and IoT approaches to integrating and monitoring construction machinery should be further studied and explored.

ACKNOWLEDGMENT

The work presented in this paper was financed by Conduril, the UT Austin – Portugal Program / INESC TEC. It was also funded by Guangzhou University in the context of Alliance Joint Research and Publication Projects, and FCT - Foundation for Science and Technology, I.P./MCTES through national funds (PIDDAC), within the scope of CISUC R&D Unit - UIDB/00326/2020 or project code UIDP/00326/2020.

REFERENCES

[1] C. Zhang, J. He, C. Bai, X. Yan, J. Gong, and H. Zhang, "How to use advanced fleet management system to promote energy saving in transportation: A survey of drivers' awareness of fuel-saving factors," *J. Adv. Transp.*, vol. 2021, pp. 1–19, Jul. 2021.

[2] M. M. Vazifeh, P. Santi, G. Resta, S. H. Strogatz, and C. Ratti, "Addressing the minimum fleet problem in on-demand urban mobility," *Nature*, vol. 557, no. 7706, pp. 534–538, May 2018. [Online]. Available: https://www.nature.com/articles/s41586-018-0095-1

[3] P. Kopelias, E. Demiridi, K. Vogiatzis, A. Skabardonis, and V. Zafiropoulou, "Connected & autonomous vehicles—Environmental impacts—A review," *Sci. The Total Environ.*, vol. 712, Apr. 2020, Art. no. 135237.

[4] V. K. Kukkala, J. Tunnell, S. Pasricha, and T. Bradley, "Advanced driver-assistance systems: A path toward autonomous vehicles," *IEEE Consum. Electron. Mag.*, vol. 7, no. 5, pp. 18–25, Sep. 2018.

[5] U. Montanaro, S. Dixit, S. Fallah, M. Dianati, A. Stevens, D. Oxtoby, and A. Mouzakitis, "Towards connected autonomous driving: Review of use-cases," *Vehicle Syst. Dyn.*, vol. 57, pp. 779–814, Jun. 2018, doi: 10.1080/00423114.2018.1492142.

[6] K. Kiela, V. Barzdenas, M. Jurgo, V. Macaitis, J. Rafanavicius, A. Vasjanov, L. Kladovscikov, and R. Navickas, "Review of V2X–IoT standards and frameworks for ITS applications," *Appl. Sci.*, vol. 10, no. 12, p. 4314, Jun. 2020. [Online]. Available: https://www.mdpi.com/2076-3417/10/12/4314/htm

[7] Y. Guang, L. Dongbo, and M. Chaofeng, "Design and implementation of roadside intelligent information interaction system based on edge computing," *J. Phys., Conf.*, vol. 1486, no. 2, Apr. 2020, Art. no. 022022, doi: 10.1088/1742-6596/1486/2/022022.

[8] M. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, Jun. 2022.

[9] S. Chen, J. Hu, Y. Shi, L. Zhao, and W. Li, "A vision of C-V2X: Technologies, field testing, and challenges with Chinese development," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3872–3881, May 2020.

[10] K. Petroutsatou and P. Giannoulis, "Analysis of construction machinery market: The case of Greece," *Int. J. Construct. Manage.*, vol. 22, no. 9, pp. 1667–1674, Jul. 2022, doi: 10.1080/15623599.2020.1741491.

[11] E. Forcael, I. Ferrari, A. Opazo-Vega, and J. A. Pulido-Arcas, "Construction 4.0: A literature review," *Sustainability*, vol. 12, no. 22, p. 9755, 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/22/9755/htm

[12] C. Yizhan, W. Zhong, H. Da, and L. Ruosen, "6G is coming : Discussion on key candidate technologies and application scenarios," in *Proc. Int. Conf. Comput. Commun. Netw. Secur. (CCNS)*, Aug. 2020, pp. 59–62.

[13] E. Sisinni and A. Mahmood, "Wireless communications for industrial Internet of Things: The LPWAN solutions," in *Wireless Networks and Industrial IoT*. Cham, Switzerland: Springer, 2021, pp. 79–103. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-51473-0_5

[14] M. Bozdal, M. Samie, and I. Jennions, "A survey on can bus protocol: Attacks, challenges, and potential solutions," in *Proc. Int. Conf. Comput., Electron. Commun. Eng. (iCCECE)*, Aug. 2018, pp. 201–205.

[15] P. K. R. Maddikunta, Q.-V. Pham, P. B, N. Deepa, K. Dev, T. R. Gadekallu, R. Ruby, and M. Liyanage, "Industry 5.0: A survey on enabling technologies and potential applications," *J. Ind. Inf. Integr.*, vol. 26, Mar. 2022, Art. no. 100257.

[16] R. N. Gore, H. Kour, M. Gandhi, D. Tandur, and A. Varghese, "Bluetooth based sensor monitoring in industrial IoT plants," in *Proc. Int. Conf. Data Sci. Commun. (IconDSC)*, Mar. 2019, pp. 1–6.

[17] I.-G. Lee, D. B. Kim, J. Choi, H. Park, S.-K. Lee, J. Cho, and H. Yu, "WiFi HaLow for long-range and low-power Internet of Things: System on chip development and performance evaluation," *IEEE Commun. Mag.*, vol. 59, no. 7, pp. 101–107, Jul. 2021.

[18] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh, and J. Nayak, "Industrial Internet of Things and its applications in industry 4.0: State of the art," *Comput. Commun.*, vol. 166, pp. 125–139, Jan. 2021.

[19] A. Khalifeh, K. A. Aldahdouh, K. A. Darabkh, and W. Al-Sit, "A survey of 5G emerging wireless technologies featuring LoRaWAN, Sigfox, NB-IoT and LTE-M," in *Proc. Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET)*, Mar. 2019, pp. 561–566.

[20] M. Ballerini, T. Polonelli, D. Brunelli, M. Magno, and L. Benini, "NB-IoT versus LoRaWAN: An experimental evaluation for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7802–7811, Dec. 2020.

[21] N. Tsavalos and A. A. Hashem. (2018). *Low Power Wide Area Network (LPWAN) Technologies for Industrial IoT Applications*. [Online]. Available: https://lup.lub.lu.se/student-papers/record/8950859/file/8950964.pdf

[22] M. Dangana, S. Ansari, Q. H. Abbasi, S. Hussain, and M. A. Imran, "Suitability of NB-IoT for indoor industrial environment: A survey and insights," *Sensors*, vol. 21, no. 16, p. 5284, Aug. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/16/5284/htm

[23] D. Raposo, A. Rodrigues, S. Sinche, J. S. Silva, and F. Boavida, "Securing wirelessHART: Monitoring, exploring and detecting new vulnerabilities," in *Proc. IEEE 17th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Nov. 2018.

[24] A. Mahmood, S. F. Abedin, T. Sauter, M. Gidlund, and K. Landernas, "Factory 5G: A review of industry-centric features and deployment options," *IEEE Ind. Electron. Mag.*, vol. 16, no. 2, pp. 24–34, Jun. 2022.

[25] S. Sinche, D. Raposo, N. Armando, A. Rodrigues, F. Boavida, V. Pereira, and J. S. Silva, "A survey of IoT management protocols and frameworks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1168–1190, 2020.

[26] D. Raposo, A. Rodrigues, S. Sinche, J. Sá Silva, and F. Boavida, "Industrial IoT monitoring: Technologies and architecture proposal," *Sensors*, vol. 18, no. 10, p. 3568, Oct. 2018. [Online]. Available: https://www.mdpi.com/journal/sensors

[27] E. Safrianti, L. O. Sari, and N. A. Sari, "Real-time network device monitoring system with simple network management protocol (SNMP) model," in *Proc. 3rd Int. Conf. Res. Academic Community Services (ICRACOS)*, Oct. 2021, pp. 122–127.

[28] S. Rao, D. Chendanda, C. Deshpande, and V. Lakkundi, "Implementing LWM2M in constrained IoT devices," Inst. Electr. Electron. Eng., Tech. Rep., 2016, pp. 52–57.

[29] J. Schonwalder, M. Bjorklund, and P. Shafer, "Network configuration management using NETCONF and Yang," *IEEE Commun. Mag.*, vol. 48, no. 9, pp. 166–173, Sep. 2010.

[30] J. De C. Silva, J. José P. C. Rodrigues, K. Saleem, S. A. Kozlov, and R. A. L. Rabêlo, "M4DN.IoT–A networks and devices management platform for Internet of Things," *IEEE Access*, vol. 7, pp. 53305–53313, 2019.

[31] S. Sinche, J. S. Silva, D. Raposo, A. Rodrigues, V. Pereira, and F. Boavida, "Towards effective IoT management," in *Proc. IEEE SENSORS*, New Delhi, India, Dec. 2018.

[32] D. Raposo, A. Rodrigues, S. Sinche, J. S. Silva, and F. Boavida, "Security and fault detection in in-node components of IIoT constrained devices," in *Proc. Conf. Local Comput. Netw. (LCN)*, Oct. 2019, pp. 282–290.

[33] G. Codeluppi, A. Cilfone, L. Davoli, and G. Ferrari, "VegIoT garden: A modular IoT management platform for urban vegetable gardens," in *Proc. IEEE Int. Workshop Metrology Agricult. Forestry (MetroAgriFor)*, Oct. 2019, pp. 121–126.
[34] P. Killeen, B. Ding, I. Kiringa, and T. Yeap, *IoT-Based Predictive Maintenance for Fleet Management*, vol. 151. Amsterdam, The Netherlands: Elsevier, 2019, pp. 607–613.
[35] C. Boudagdigue, A. Benslimane, A. Kobbane, and J. Liu, "Trust management in industrial Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3667–3682, 2020.
[36] P. Moens, V. Bracke, C. Soete, S. Vanden Hautte, D. Nieves Avendano, T. Ooijevaar, S. Devos, B. Volckaert, and S. Van Hoecke, "Scalable fleet monitoring and visualization for smart machine maintenance and industrial IoT applications," *Sensors*, vol. 20, no. 15, p. 4308, Aug. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/15/4308/htm
[37] A. Zahra, M. Asif, A. A. Nagra, M. Azeem, and S. A. Gilani, "Vulnerabilities and security threats for IoT in transportation and fleet management," in *Proc. 4th Int. Conf. Comput. Inf. Sci. (ICCIS)*, Nov. 2021, pp. 1–5.
[38] H. Aguirre-Jofré, M. Eyre, S. Valerio, and D. Vogt, "Low-cost Internet of Things (IoT) for monitoring and optimising mining small-scale trucks and surface mining shovels," *Autom. Construct.*, vol. 131, Nov. 2021, Art. no. 103918.
[39] K. S. Praveena, M. Prajwal, K. Bhargavi, and M. R. Darshan, "An automatic overloaded vehicle monitoring and prevention system using IoT," in *Proc. Int. Conf. Recent Trends Electron., Inf., Commun. Technol. (RTEICT)*, Aug. 2021, pp. 788–792.
[40] R. Silapunt, W. Panpanyatep, and G. Boonsothonsatit, "Design and development of the smart object for the IoT-enabled smart warehouse," in *Proc. Int. Electr. Eng. Congr. (iEECON)*, Mar. 2022, pp. 1–2.
[41] W. Voss, *A Comprehensible Guide to J1939*. Amherst, MA, USA: Copperhill Technologies Corporation, 2008.
[42] S. Dilakshan, A. P. Rathnasinghe, and L. D. P. Seneviratne, "Potential of Internet of Things (IoT) in the construction industry," in *Proc. World Construct. Symp.*, pp. 445–457, 2021.
[43] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.
[44] J. Kiljander, A. D'Elia, F. Morandi, P. Hyttinen, J. Takalo-Mattila, A. Ylisaukko-Oja, J. P. Soininen, and T. S. Cinotti, "Semantic interoperability architecture for pervasive computing and Internet of Things," *IEEE Access*, vol. 2, pp. 856–873, 2014.
[45] N. Bahri, S. Saadaoui, M. Tabaa, M. Sadik, and H. Medromi, "Wireless technologies and applications for industrial Internet of Things: A review," in *Advances in Intelligent Systems and Computing*, vol. 1188. Singapore: Springer, 2021, pp. 505–516.
[46] M. Iqbal, A. Y. M. Abdullah, and F. Shabnam, "An application based comparative study of LPWAN technologies for IoT environment," in *Proc. IEEE Region 10 Symp. (TENSYMP)*, Jun. 2020, pp. 1857–1860.
[47] L. Kolobe, B. Sigweni, and C. K. Lebekwe, "Systematic literature survey: Applications of LoRa communication," *Int. J. Elect. Comput. Eng.*, vol. 10, pp. 3176–3183, Jun. 2020.
[48] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.
[49] H. H. R. Sherazi, L. A. Grieco, M. A. Imran, and G. Boggia, "Energy-efficient LoRaWAN for industry 4.0 applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 891–902, Feb. 2021.
[50] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Athens, Greece, Oct. 2018, pp. 197–202.
[51] R. S. Sinha, Y. Wei, and S. H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," ICT Exp., Korean Inst. Commun. Inf. Sci., South Korea, Mar. 2017, pp. 14–21, vol. 3.
[52] Y. Chen, Y. A. Sambo, O. Onireti, and M. A. Imran, "A survey on LPWAN-5G integration: Main challenges and potential solutions," *IEEE Access*, vol. 10, pp. 32132–32149, 2022.
[53] S. Moghanian, F. B. Saravi, G. Javidi, and E. O. Sheybani, "GOAMLP: Network intrusion detection with multilayer perceptron and grasshopper optimization algorithm," *IEEE Access*, vol. 8, pp. 215202–215213, 2020.
[54] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, "A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 88–122, 2022.
[55] M. Rizzi, P. Ferrari, A. Flammini, E. Sisinni, and M. Gidlund, "Using LoRa for industrial wireless networks," in *Proc. IEEE 13th Int. Workshop Factory Commun. Syst. (WFCS)*, Trondheim, Norway, Jul. 2017.
[56] E. H. Currie, "Microcontroller subsystems," in *Mixed-Signal Embedded Systems Design*. Cham, Switzerland: Springer, 2021, pp. 35–97. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-70312-7_2
[57] E. Raj, M. Westerlund, and L. Espinosa-Leal, "Reliable fleet analytics for edge IoT solutions," 2021, *arXiv:2101.04414*.

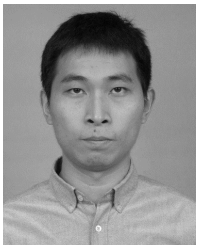
OSCAR TORRES SANCHEZ (Student Member, IEEE) received the degree in electronic and telecommunications engineering from the National Polytechnic School (Ecuador), in 2018. He is currently pursuing the Ph.D. degree with the Department of Informatics Engineering, University of Coimbra, Portugal. He is also a Researcher with the Centre for Informatics and Systems (CISUC), University of Coimbra. His research interests include the Internet of Things (IoT), the Industrial Internet of Things (IIoT), machine to machine, wireless sensors networks, and security.

DUARTE RAPOSO received the M.Sc. and Ph.D. degrees in information science and technology from the University of Coimbra, in 2012 and 2020, respectively. In 2012, he joined CISUC as a Researcher working in industrial wireless sensor networks in the topics of network management and security, exploring state-of-the-art anomaly detection techniques. In the same year, he also joined eneida.io developing industrial wireless solutions in the fields of oil and gas, mining, and energy. Since 2020, he has been with the Instituto de Telecomunicações, Aveiro, Portugal, as a Research Assistant in the network architectures and protocols. Until now, he is the author/coauthor of more than 34 scientific works in international conferences and journals and two national patents. His current research interests include wireless communications, deterministic networks, cellular communications, software-defined networks, and edge computing and orchestration.

ANDRÉ RODRIGUES received the B.Sc. degree in informatics engineering from the University of Coimbra, Portugal, the M.Sc. degree in finance from ISCTE Business School, and the Ph.D. degree in informatics engineering from the University of Coimbra, in 2013. He is currently a Researcher at the Centre of Informatics and Systems of the University of Coimbra (CISUC). He works as a Teacher at the Polytechnic Institute of Coimbra, giving classes on networking. His research interests include industrial wireless sensor networks, people-centric Internet of Things, and network management. He is the author of several papers in international journals and conferences in those areas. He has been serving as a reviewer in top conferences and participated in several European initiatives and projects. For more information visit the link (www.researchgate.net/profile/Andre-Rodrigues9).

FERNANDO BOAVIDA received the Ph.D. degree in informatics engineering, in 1990. He is currently a Full Professor at the Department of Informatics Engineering (DEI), Faculty of Sciences and Technology, University of Coimbra. His research interests include people-centric Internet of Things, cryptography, and privacy. He is the author/coauthor of more than 200 international publications (books, book chapters, refereed journals, and conference proceedings) and 50 national publications. He has participated in several European projects, such as FP6 E-NEXT, EuQoS (IST-FP6-2004-004503), WEIRD (IST-FP6 Integrated Project 034622), OpenNet (IST-FP6 Specific Support Action 035185), CONTENT (IST-FP6-0384239), GINSENG (ICT-FP7-224282), MICIE (ICT-FP7-225353), and POSEIDON (786713, H2020-DS-2016-2017/DS-08-2017). He is the author of one international book, and five textbooks in Portuguese widely used as course books in universities and polytechnic schools of Portuguese-speaking countries, in the areas of computer networks engineering, computer networks administration, TCP/IP networking, and wireless sensor networks.

RADU MARCULESCU (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of Southern California, in 1998. He is currently a Professor and the Laura Jennings Turner Chair of Engineering with the Department of Electrical and Computer Engineering, The University of Texas at Austin. From 2000 to 2019, he was a Professor with the Electrical and Computer Engineering Department, Carnegie Mellon University. His current research interests include developing new ML/AI methods and tools for modeling, analysis, and optimization of embedded systems, cyber-physical systems, social networks, and the Internet of Things.



KONGYANG CHEN received the Ph.D. degree in computer science from the University of Chinese Academy of Sciences, China. He is currently an Associate Professor with the Institute of Artificial Intelligence and Blockchain, Guangzhou University, China. From 2014 to 2018, he was an Assistant Professor at the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China. He is also the Director of Institutes of Artificial Intelligence Application, Guangzhou University, and the Associate Director of the Guangdong Provincial Engineering and Technology Research Center for Big Data Security and Privacy Preservation. His research interests include the Internet of Things, edge computing, artificial intelligence, and blockchain. He has published over 30 papers in top conferences or journals, such as IEEE INFOCOM, ACM MobiSys, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and *ACM TOSN*.

JORGE SÁ SILVA (Senior Member, IEEE) received the Ph.D. degree in informatics from the University of Coimbra, in 2001. He is currently an Associate Professor with Habilitation at the Department of Electrical and Computer Engineering (DEEC), University of Coimbra, where he is also a Researcher with the Institute for Systems Engineering and Computers at Coimbra (INESC Coimbra). His research interests include the Internet of Things, network protocols, and human in the loop. He is a Licensed Professional Engineer. For more information visit the link (https://home.deec.uc.pt/~sasilva).