CHEMICAL ENGINEERING TRANSACTIONS

VOL. 91, 2022

A publication of

AIDIC

The Italian Association
of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Valerio Cozzani, Bruno Fabiano, Genserik Reniers
Copyright © 2022, AIDIC Servizi S.r.l.
ISBN 978-88-95608-89-1; **ISSN** 2283-9216

DOI: 10.3303/CET2291044

On Safety Enhancement in IIoT Scenarios through Heterogeneous Localization Techniques

Luca Davoli[a,*], Laura Belli[a], Francesco Denaro[a], Dinesh Tamang[b], Andrea Abrardo[b], Gianluigi Ferrari[a]

[a]Internet of Things (IoT) Lab, Department of Engineering and Architecture, University of Parma, Parma, Italy
[b]Department of Information Engineering and Applied Mathematics, University of Siena, Siena, Italy
luca.davoli@unipr.it

In the field of the Industrial Internet of Things (IIoT), strictly related to Industry 4.0, one of the main aspects to be carefully considered by the governing board of a manufacturing company is the safety level to be guaranteed to the workers inside production plants. This involves daily human activities, together with production machines to be used during the working hour (and periodically maintained), and mobile industrial vehicles moving around the production plant. To this end, a precise localization of both workers and vehicles is expedient to improve the safety level—avoiding that people move inside forbidden areas or perform dangerous actions—as well as allowing a more accurate control and reporting to national authorities in charge of verifying the compliance to safety regulations (e.g., aggregated data, not shared outside the company, used to fill injuries reports in case of official inspections), in the presence of accidents and anomalous events. In this paper, we present the design of IIoT-related localization mechanisms exploiting heterogeneous communication technologies, in turn analysing how the localization can cope with the adoption of wideband (e.g., Wi-Fi) and narrowband (e.g., Narrowband IoT, NB-IoT) communication protocols and discussing how these communication paradigms may impact existing and modern production plants.

1. Introduction

One of the paradigms uprising in the last decade in the manufacturing domain is the Industrial Internet of Things (IIoT), strictly related to Industry 4.0, which represents one of the key building blocks of smart industrial applications, leveraging next-generation Cyber-Physical Systems (CPSs), which are radically changing many business models (Belli *et al.*, 2019; Xu *et al.*, 2014). Nowadays, almost any productive sector can rely on the use of smart sensing and actuating devices, enabling access to far greater information, with enhanced reliability, efficiency, and accuracy (Deng *et al.*, 2018). At the same time, there is a strong need to increase the safety in working environments (Palattella *et al.*, 2016). In fact, an important aspect for IIoT systems monitoring industrial processes is represented by technologies helping in protecting people working in plants where accidents happen (Andreu, 2020), with safety being enhanced by knowing the position of workers and machines inside industrial environments.

Safety on workplaces is a key objective of the IIoT paradigm, as it safeguards people in all potentially risky areas (such as oil and gas plants, and chemical industries) where accidents due to dangerous event or action might be prevented—as an example, localization of workers or vehicles to avoid access to forbidden areas. Furthermore, maintaining a safe environment in industrial contexts has several legal implications (i.e., taking measures to adhere to safety standards and regulations, using aggregated data, not shared outside the company, to fill injuries reports in case of official inspections), that must be considered to exploit proper reporting systems built on top of IIoT mechanisms (e.g., through the blockchain paradigm (Bodkhe, 2020; Davoli *et al.*, 2020) against data's theft and damage (Wadsworth *et al.*, 2019)). Besides the "general" objectives of Industry 4.0 in production scenarios, communications between several IIoT devices (Machine-to-Machine, M2M, approach) and with people (Human-to-Machine, H2M, approach) represent a challenging aspect. To this end, it is important to understand how network architectures, based on public or private infrastructures for future IoT scenarios, exploiting Fog/Edge/Cloud Computing, and using low (e.g.,

Paper Received: 9 January 2022; Revised: 18 March 2022; Accepted: 17 May 2022
Please cite this article as: Davoli L., Belli L., Denaro F., Tamang D., Abrardo A., Ferrari G., 2022, On Safety Enhancement in Iiot Scenarios Through Heterogeneous Localization Techniques, Chemical Engineering Transactions, 91, 259-264 DOI:10.3303/CET2291044

LoRaWAN) and high (e.g., 4G/5G) data rate communication technologies (Lin *et al.*, 2019) can be employed for localization and work safety purposes.

The goal of generic localization systems is to estimate the position of targets moving in a monitored environment. To this end, they can be divided into two main classes: (i) *indoor* localization systems, if targets move inside an indoor environment; and (ii) *outdoor* localization systems, when targets are moving in an open space. In this latter class of scenarios, it is usually possible to employ satellite-based localization technologies such as Global Navigation Satellite System (GNSS) and Real Time Kinematic (RTK). Moreover, indoor and outdoor localization strategies significantly differ in terms of requirements, constraints and exploitable technologies. A hybrid approach, considering a continuous monitoring of a target moving in a mixed indoor/outdoor environment, is a challenging topic, not yet fully analysed in literature.

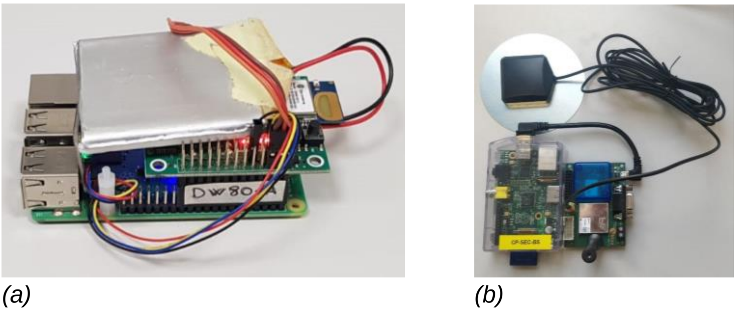
Motivated by the considerations above, in this paper an IIoT safety and monitoring infrastructure targeting both indoor and outdoor industrial scenarios is proposed. The system is composed by prototypical nodes, integrating Commercial Off-The-Shelf (COTS) components, and implementing custom algorithms to estimate the position of indoor and outdoor targets, which is sent to a remote server via wireless communication protocols. The proposed IIoT infrastructure aims at integrating heterogeneous technologies for improving the overall localization accuracy and providing a rapid monitoring platform for enhancing safety in workplaces. The targets are located in potentially dangerous working environments, where localization is important to detect workers and industrial vehicles accessing forbidden areas, thus issuing alarms accordingly.

The rest of the paper is organized as follows. In Section 2, the proposed IIoT-oriented indoor and outdoor localization system is presented. Section 3 discusses on experimental performance evaluations of the proposed IIoT safety infrastructure. Finally, in Section 4 conclusions are drawn.

2. Proposed Architecture

The indoor localization system for the proposed IIoT safety architecture is based on the integration of two different heterogeneous technologies: Ultra-Wideband (UWB) and Inertial Measurement Units (IMUs). More in detail, the target corresponds to a custom IoT device equipped with a UWB tag and an IMU, while the monitored environment is covered with N UWB anchors, with $N \geq 2$. Then, the indoor localization algorithm estimates the target's position by fusing the orientation information given by the IMU and the ranging data obtained by UWB anchors interacting with the UWB tag.

Figure 1a shows the indoor IIoT node prototype based on a Raspberry Pi 3 Model B+ (RPi3) connected with a Decawave DWM1001 module (Decawave, 2021) as UWB tag, and a Bosch BNO055 (Bosch, 2021) IMU sensor. A Python-based application has been developed to fuse data collected from both UWB tag and IMU.



(a) *(b)*

Figure 1: (a) IIoT node prototype for indoor localization. (b) IIoT node prototype (able to work both as base station and as rover) for outdoor localization.

Instead, the outdoor localization system has been developed leveraging satellite positioning technologies, such as GNSS and RTK. A GNSS localization system can be considered as "stand-alone," while RTK systems involve an infrastructure composed by a *base station*, corresponding to a fixed station whose coordinates are known, which interacts with a *rover*, corresponding to the mobile target to be localized. With respect to the "pure" GNSS solution, the RTK enhances rover's position precision through corrections received from the base station (via a RTCM3 message exchange (ESA, 2021)), with a final positioning status that, based on environmental conditions and amount of visible satellites, may pertain to one of the following classes: (i) *autonomous*, when the rover is not able to receive corrections from the base station, so the positioning is given only by GNSS; (ii) *float*, if the rover receives information from the base station, while not having a sufficient number of visible satellites; and (iii) *fixed*, in which both the rover and the base station observe a sufficient amount of shared satellites, obtaining the maximum precision (1÷5 cm in ideal conditions). If not known, the base station’s coordinates can be retrieved through a *survey-in* procedure, requiring a certain observation time and processing of the retrieved satellites information.

The outdoor localization system prototype, shown in Figure 1b, is similar for both base station and rover. More in detail, they are both based on a RPi3 processing node, connected with a u-blox C94-M8P RTK board (u-blox, 2021a), based on the NEO-M8P-2 chip and compatible with BeiDou, GLONASS, and GPS/QZSS positioning systems. The u-blox modules include a UHF antenna, to exchange RTCM3 messages, and a GNSS antenna to receive satellites data. While the base station is powered through the main power supply (since it is fixed and needs to act as a reliable and “always-on” reference), the rover is powered with a battery pack, dimensioned to respect the expected duration (e.g., a complete working day). The software running on the RPi3 is a Python-based application developed to process data collected from the external antennas. On the base station the application may run both in *fixed* and *survey-in* modes, while on the rover the application can handle both GNSS and RTK positioning, switching to RTK operational mode when the base station sends corrections, and to manage u-blox-compliant messages and parse NMEA-compliant localization messages (u-blox, 2021b).

In IoT applications, wireless communication protocols are extremely heterogeneous and, therefore, one needs to evaluate the ones better fitting the specific application context. In the proposed IIoT safety scenario, the communication protocol requirements to transfer people and vehicles’ localization data are: (i) medium/long-range coverage, (ii) adaptability to indoor and outdoor environments, (iii) sustainable energy consumption, and (iv) data rate compatible with a moving vehicle. To this end, several communication protocols have been evaluated, including long-range communications (e.g., LoRaWAN and Narrowband IoT, NB-IoT, but also 4G/5G cellular communications with higher data rate), and medium-range communications (e.g., Wi-Fi, Bluetooth and Bluetooth Low Energy, BLE, all of them allowing a high transmission data rate). Considering the requirements of the targeted IIoT scenarios (Cilfone *et al.*, 2019), in the proposed IIoT system the Wi-Fi protocol has been chosen for both indoor and outdoor contexts. In particular, data are sent from localization devices to a remote server, in charge of processing information, through HTTP REST APIs. This solution allows to obtain high interoperability, reliability and security in the communication without duty cycle and data rate constraints. Figure 2 shows the indoor and outdoor localization communication pattern among the proposed IIoT infrastructure’s components, thus highlighting how additional safety nodes (e.g., environmental sensors adopting low data rate communication protocols) may be easily integrated.

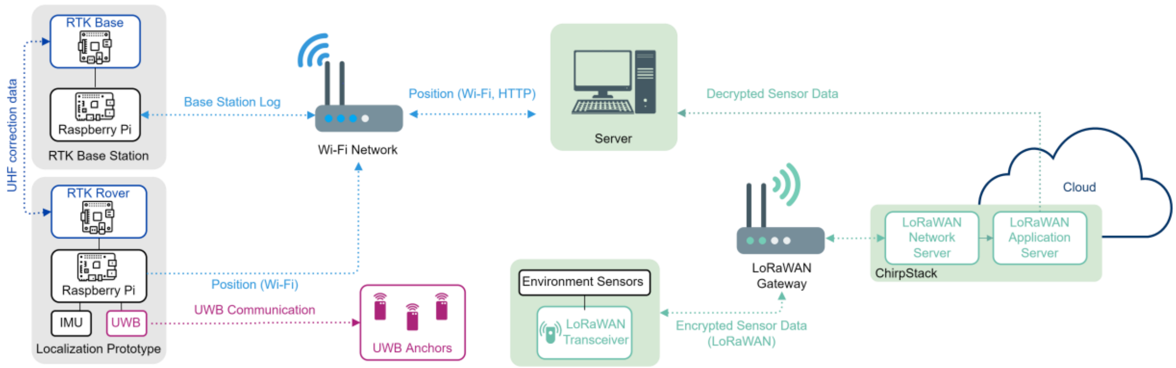


Figure 2: Communication pattern among the IIoT nodes involved in the proposed safety infrastructure.

3. Experimental Results

In order to verify how the proposed prototypical IIoT localization infrastructure performs, experimental campaigns have been carried out including both indoor and outdoor environments.

One of the main objectives of the experimental characterization of indoor localization is to identify the anchors’ configuration needed to obtain a good accuracy (namely, localization error below 0.5 m) with the minimum number of UWB anchors in the environment, leveraging the additional information given by the IMU. Several experimental campaigns have been performed in the Department of Engineering and Architecture of the University of Parma, Parma, Italy. In particular, we deployed Decawave DWM1011 UWB anchors, located at a 2 m height, over the walls of an internal long (200 m) corridor, while the target node has been located on a transport trolley at a 15 cm height from the ground. The experimental results in the indoor scenario are shown in Figure 3, Figure 4, and Figure 5, where: red markers represent the UWB anchors deployed in the corridor;

black arrows identify the real path followed by the mobile target; and blue markers correspond to the path estimated by the indoor localization algorithm.

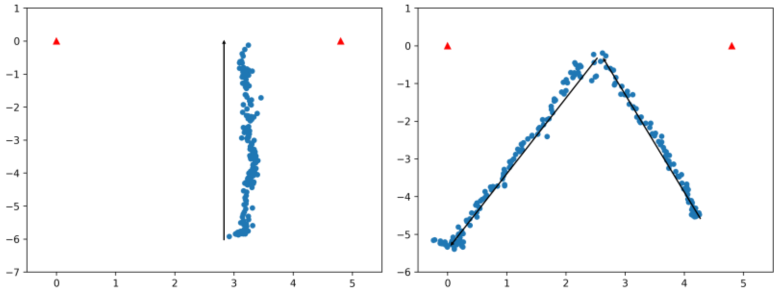


Figure 3: Experimental performance of the indoor localization algorithm with two UWB anchors. Two illustrative paths (real paths are indicated by solid lines) are shown.

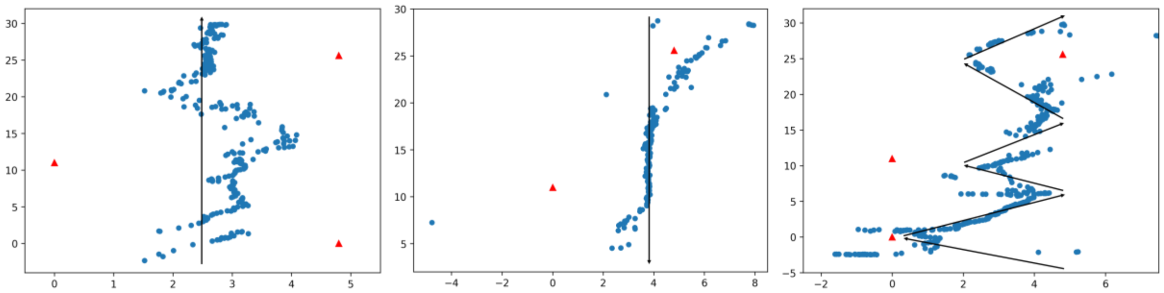


Figure 4: Experimental performance of the indoor localization algorithm with three UWB anchors. Three illustrative paths (real paths are indicated by solid lines) are shown.

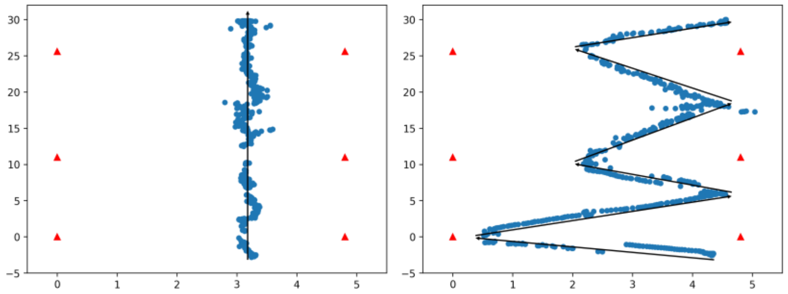


Figure 5: Experimental performance of the indoor localization algorithm with six UWB anchors in grid. Two illustrative paths (real paths are indicated by solid lines) are shown.

Figure 3 highlights how two UWB anchors deployed frontally in a narrow environment allow to obtain a good reconstruction of the path when the target remains inside the anchors' coverage area. Figure 4 shows that with three UWB anchors positioned apart from and not in front of each other (in such a way that when the target is moving, only two UWB anchors are in visibility range), the path reconstruction is inaccurate. This suggests that UWB anchors' positioning has a strong impact on the performance, especially when the target is close to the UWB anchors' operational limit (around 10 m). Finally, Figure 5 shows that with anchors deployed in a grid topology (with each pair of anchors in front of each other), the precision significantly increases, thus confirming that a grid anchors' deployment should be preferred in indoor scenarios.

Considering the outdoor localization performance estimation, a first evaluation has been performed placing the base station node at a 3 m height over a box rooftop (without significant nearby obstacles), as depicted in Figure 6a, and running a *survey-in* procedure which lasted approximately 7 hours with a 30 cm position on single coordinate precision. In Figure 6b a comparison between the path estimation performance with GNSS and RTK systems in an outdoor environment is shown. The obtained localization errors are in the range 80÷180 cm with the GNSS, and in the range 25÷60 cm with the RTK system.

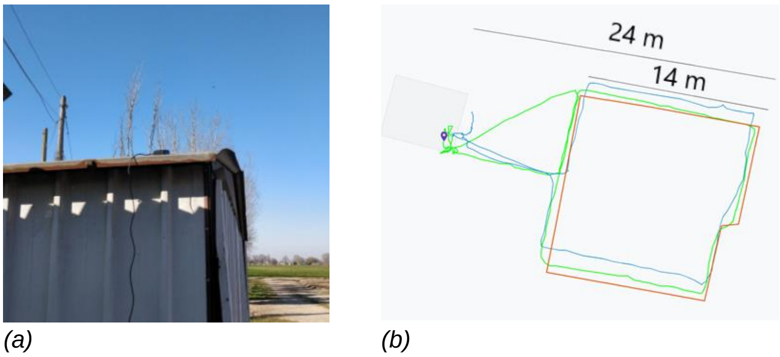


Figure 6: (a) Deployment of the base station. (b) Comparison between real (orange line) and estimated (blue line with GNSS; green line with RTK) paths.

In order to estimate how the external GNSS antenna can influence the localization results, another experimental campaign has been conducted employing a more precise Taoglas MA130 one (Taoglas, 2021). The base station has been located over a metallic base (to improve signals reception) and, then, a 470 m walking path (with some obstacles present, such as trees and buildings) has been considered, maintaining the rover's antenna at a 1.5 m height and reaching a maximum base station-rover distance of about 110 m.

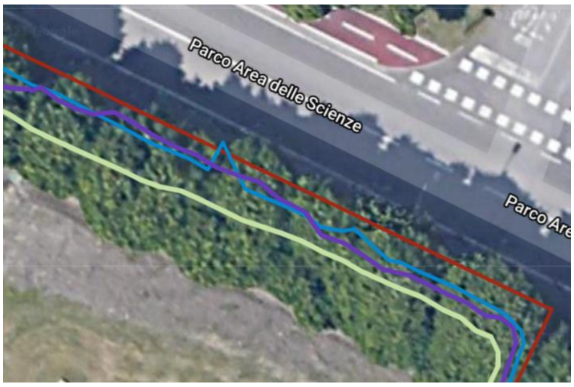


Figure 7: Comparison between real (red line) and estimated paths with different GNSS antennas (green for GNSS only; purple for RTK with Taoglas antenna; blue for RTK with generic GNSS antenna).

In Figure 7 the red line corresponds to the target real path, the green line represents the localization result using GNSS information, the purple line represents the path estimated in RTK mode with a Taoglas antenna, and the blue line represents the path estimated in RTK mode with a generic GNSS antenna. A localization accuracy of 1 m has been achieved with GNSS, while an accuracy of about 40 cm has been obtained in RTK mode. The main difference among the chosen GNSS antennas is that the Taoglas MA130 provides a better and more stable and lasting RTK *fixed* mode rather than the generic antenna.

4. Conclusions and Future Works

In this paper, an IIoT-oriented indoor and outdoor localization system, targeting industrial environments, has been presented. The prototypical devices composing the safety-oriented system feature a central processing board, equipped with sensors and communication interfaces. Experimental performance analysis has been performed in different environments, highlighting (i) how a correct deployment of reference elements in the monitored environment is a crucial aspect, as well as (ii) how obstacles may interfere with data transmission between target devices and remote (in the Edge/Cloud) decision support platforms. As future works, the proposed IIoT infrastructure might be updated to unify the indoor and outdoor localization nodes in a unique final IIoT device. This device may also be extended, e.g., by integrating additional ultrasonic sensors (Davoli *et al.*, 2021), to extend indoor localization data fusion, improving obstacles identification in the absence of more reliable mechanisms. The adoption of *wearable* systems, to be worn by the entity to be monitored through the RTK rover, is also an attractive research extension.

Nomenclature

BLE – Bluetooth Low Energy
COTS – Commercial Off-The-Shelf
CPS – Cyber-Physical System
GNSS – Global Navigation Satellite System
H2M – Human-to-Machine
IIoT – Industrial Internet of Things
IMU – Inertial Measurement Unit
M2M – Machine-to-Machine
NB-IoT – Narrowband IoT
RPi3 – Raspberry Pi 3
RTK – Real Time Kinematic
UWB – Ultra-WideBand

Acknowledgments

This work was supported by the National Institute for Insurance against Accidents at Work ("Istituto Nazionale Assicurazione Infortuni sul Lavoro", INAIL), under “Bando Ricerche In Collaborazione” (BRIC) 2019, Piano Attività di ricerca 2019-2021, Tematica n. 2 “Approcci integrati e metodologie innovative per la prevenzione del fenomeno infortunistico anche attraverso l’analisi dei near miss,” “Sistema Cyber-Fisico per la sicurezza in stabilimenti a rischio incidenti rilevanti con integrazione di tecnologie di localizzazione di persone e mezzi e di sistemi di sensori distribuiti” (CP-SEC) project.

References

Andreu A., 2020, Operational Technology Security – A Data Perspective, Network Security, 2020(1), 8–13. doi:10.1016/S1353-4858(20)30008-8.

Belli L., Davoli L., Medioli A., Marchini P.L., Ferrari G., 2019, Toward Industry 4.0 With IoT: Optimizing Business Processes in an Evolving Manufacturing Factory, Frontiers in ICT, 6. doi:10.3389/fict.2019.00017.

Bodkhe U., Tanwar S., Parekh K., Khanpara P., Tyagi S., Kumar N., Alazab M., 2020, Blockchain for Industry 4.0: A Comprehensive Review, IEEE Access, 8, 79764–79800. doi:10.1109/ACCESS.2020.2988579.

Bosch, 2021, BNO055 <www.bosch-sensortec.com/products/smart-sensors/bno055/> accessed 14.12.2021.

Cilfone A., Davoli L., Belli L., Ferrari G., 2019, Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies, Future Internet, 11(4). doi:10.3390/fi11040099.

Davoli L., Belli L., Ferrari G., 2020, IoT-enabled Smart Monitoring and Optimization for Industry 4.0, Chapter In: Atzori L., Ferrari G. (Eds.), Internet of Things: Technologies, Challenges and Impact, 5, 207–226.

Davoli L., Paraskevopoulos I., Campanella C., Bauro S., Vio T., Abrardo A., Ferrari G., 2021, Ultrasonic-Based Environmental Perception for Mobile 5G-Oriented XR Applications, Sensors, 21(4). doi:10.3390/s21041329.

Decawave, 2021, DWM1001 Development Board, <www.decawave.com/product/dwm1001-development-board/> accessed 14.12.2021.

Deng X., Yang L.T., Yi L., Wang M., Zhu Z., 2018, Detecting Confident Information Coverage Holes in Industrial Internet of Things: An Energy-Efficient Perspective, IEEE Communications Magazine, 56(9), 68–73. doi:10.1109/MCOM.2018.1701195.

European Space Agency (ESA), 2021, RTK Standards, <gssc.esa.int/navipedia/index.php/RTK_Standards> accessed 14.12.2021.

Lin X., Li J., Baldemair R., Cheng J.T., Parkvall S., Larsson D.C., Koorapaty H., Frenne M., Falahati S., Grovlen A., Werner K., 2019, 5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology, IEEE Communications Standards Magazine, 3(3), 30–37. doi:10.1109/MCOMSTD.001.1800036.

Palattella M.R., Dohler M., Grieco A., Rizzo G., Torsner J., Engel T., Ladid L., 2016, Internet of Things in the 5G Era: Enablers, Architecture, and Business Models, IEEE Journal on Selected Areas in Communications, 34(3), 510–527. doi:10.1109/JSAC.2016.2525418.

Taoglas, 2021, Hercules MA130, <www.taoglas.com/product/hercules-ma130-2in1-permanent-mount-gpsglonass-868mhz-2/> accessed 14.12.2021.

u-blox, 2021, C94-M8P, <www.u-blox.com/en/product/c94-m8p> accessed 14.12.2021.

u-blox, 2021, u-blox protocol specification, <tinyurl.com/ubloxnmeamsg> accessed 14.12.2021.

Wadsworth A., Thanoon M.I., McCurry C., Sabatto S.Z., 2019, Development of IIoT Monitoring and Control Security Scheme for Cyber Physical Systems, 2019 SoutheastCon, 1–5. doi:10.1109/SoutheastCon42311.2019.9020516.

Xu L.D., He W., Li S., 2014, Internet of Things in Industries: A Survey, IEEE Transactions on Industrial Informatics, 10(4), 2233–2243. doi:10.1109/TII.2014.2300753.