information

MDPI

Article

Design of IoT-based Cyber–Physical Systems: A Driverless Bulldozer Prototype

Nelson H. Carreras Guzman [1,2,*] and Adam Gergo Mezovari [3]

[1] Engineering Systems Design Group, Technical University of Denmark (DTU), 2800 Kgs. Lyngby, Denmark
[2] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology (NTNU), 7491 Trondheim, Norway
[3] Whyyy ApS, Copenhagen K-1200, Denmark; am@whyyy.dk
* Correspondence: nelca@dtu.dk

Received: 30 September 2019; Accepted: 3 November 2019; Published: 5 November 2019

Abstract: From autonomous vehicles to robotics and machinery, organizations are developing autonomous transportation systems in various domains. Strategic incentives point towards a fourth industrial revolution of cyber–physical systems with higher levels of automation and connectivity throughout the Internet of Things (IoT) that interact with the physical world. In the construction and mining sectors, these developments are still at their infancy, and practitioners are interested in autonomous solutions to enhance efficiency and reliability. This paper illustrates the enhanced design of a driverless bulldozer prototype using IoT-based solutions for the remote control and navigation tracking of the mobile machinery. We illustrate the integration of a cloud application, communication protocols and a wireless communication network to control a small-scale bulldozer from a remote workstation. Furthermore, we explain a new tracking functionality of work completion using maps and georeferenced indicators available via a user interface. Finally, we provide a preliminary safety and security risk assessment of the system prototype and propose guidance for application in real-scale machinery.

Keywords: Internet of Things (IoT); mobile machinery; cyber-physical systems

1. Introduction

Leading the development of a fourth industrial revolution, cyber–physical systems (CPSs) are "engineered systems that integrate information technologies, real-time control subsystems, physical components and human operators to influence physical processes by means of cooperative and (semi)automated control functions" [1]. CPSs are making the remote and (semi)autonomous control of physical systems possible, integrating physical world applications with real-time communications and computational processes [2,3]. Moreover, swift advances in wireless communication technologies, embedded systems and internet pervasiveness are allowing for advances of the Internet of Things (IoT) solutions to monitor critical infrastructures and industrial activities [4]. Indeed, wireless sensor networks (WSN) integrated with IoT technologies are allowing for the continuous monitoring of the physical environment for water management, smart grids, transportation networks, and croplands, among others [5,6].

The developments in the fields of IoT and CPS are key factors leading to a fourth industrial revolution, also referred as Industry 4.0 [7,8]. In smart vehicles, their applications include autonomous cars, buses and trains for urban mobility; trucks, vessels and drones for logistics; and "mobile machinery" [9], such as tractors and heavy-duty vehicles in the agriculture, mining and construction industries. Compared to autonomous cars, driverless mobile machinery allows for simpler configurations for fleet coordination because the latter mainly operate in controlled work areas owned

by the stakeholders [10,11]. Overall, these characteristics make mobile machinery cases attractive for automation, having already been proven as economically feasible in some applications [12,13]. The current high costs of precise positioning systems (e.g., a real-time kinematic Global Positioning System (RTK GPS)) and laser vision sensors (e.g., Lidar) are being progressively reduced due to competitive innovation [14].

Assessing the technological advances in mobile machinery, Wilson [15] studied 50 years of guidance systems for agricultural vehicles and concluded that the incorporation of a global positioning system and detection sensors in a vehicle is an applicable solution to substitute human drivers. More recently, Mousazadeh [16] studied six classes of navigation systems for agricultural machinery, emphasizing central issues such as safety, economic viability and standardization. In experimental deployments, Stentz et al. [13] demonstrated a platform for automation and assessed a semi-autonomous tractor equipped with a GPS and sensors to detect obstacles and to brake to prevent collision.

Currently, innovation incentives privilege remote control and fully autonomous operations. From this perspective, Nørremark et al. [17] designed an autonomous control system to perform hoeing within crop rows without collision with plants. In the private industry, companies such as Caterpillar in the mining sector [18] and CNH Industrial in the agricultural sector [19] currently provide solutions for semi- and fully-autonomous tractors. However, none of these reviewed applications integrate IoT-based solutions to monitor and control these driverless vehicles. Overall, from this review, we assessed that researchers have mainly focused on industrial IoT-based applications for information awareness through monitoring. Furthermore, we assessed that these technologies are also suitable for integration in the automation of mobile machineries, providing a platform to monitor and remotely control them in real-time.

Therefore, this paper demonstrates an enhanced execution to remotely control a small-scale driverless bulldozer presented in [20], including a new navigation tracking function using a GPS and a new cloud architecture. We integrate a cloud application, communication protocols, and a wireless communication network to a control system in the vehicle, enabling the remote control of semi-autonomous mobile machineries from an affordable, open-source, easy-to-install and scalable platform. While focusing on the integration of different communication technologies and the cloud application, we also demonstrate the physical implementation and operation of a small-scale driverless bulldozer. Finally, we conducted a preliminary safety and security risk assessment, highlighting our recommendation to conduct this type of early stage analysis in safety-critical CPSs.

This paper is organized as follows. Section 2 describes the communication technologies surveyed, providing the reasoning to select the implemented ones. Section 3 presents the system architecture in diagrammatic representation, the physical built prototype and the developed user interface (UI). Section 4 illustrates the results of the designed prototype, including insights on a preliminary safety and security risk assessment. Section 5 suggests further developments for scaling the project, and finally Section 6 concludes.

2. Description of Communication Technologies

To realize the remote operation of the developed prototype, we needed to establish wireless communication from the bulldozer to a cloud application. Because this kind of vehicle requires reliable monitoring, the connection needed to be not only persistent but also capable of sending a sufficient amount of data with a high frequency. The applied communication technology also needed to cover wide areas to avoid limitations in the size of the work fields. The different considered communication technologies are compared in Table 1, adapted from [21–23].

Table 1. Comparison of network technologies.

Feature	Cellular (GPRS)	Wifi (802.11ah)	LoRa	Sigfox	NB-IoT
Max range	15 km	1 km	15 km	50 km	15 km
Max data rate (up/down)	20/114 kbps	7.8/7.8 Mbps	100/100 kbps	100/100 kbps	64/128 kbps
Scalability	High	Limited	Very Low	Low	High
Power need	High	High	Low	Low	Medium
Cost	Low	Medium	High	Low	Medium
Frequency band	Reserved	Open	Open	Open	Reserved

2.1. General Packet Radio Service (GPRS)

Considering the above comparison table, we selected the General Packet Radio Service (GPRS) technology, an extension of the Global System for Mobile (GSM) technology with support for data features, to connect the internet via the internet protocol suite (TCP/IP). Cellular networks provide suitable field coverage for moving vehicles. The cost of the implementation is also beneficial. With an inexpensive GSM module and a subscriber identity module (SIM) card, the client is authorized to use the well-established cellular networks of telecommunication companies. Considering data rate and scalability, cellular networks have proven to be a preferable choice. Moreover, a frequency band is reserved for this technology, making it less prone to jamming and unauthorized access. Operators manage and maintain its infrastructure, providing a reliable and secure connection.

The power consumption of a cellular module is significantly high comparing to other IoT communication technologies. However, in a real application, a diesel engine would be running the bulldozer. Therefore, power need is not a significant issue in this application. In our prototype, an SIM800L GSM module was attached to the microcontroller as a modem to connect the vehicle to the cellular network. To control the GSM modem, we used standard attention (AT) commands.

2.2. Message Queuing Telemetry Transport (MQTT)

The open-source Message Queuing Telemetry Transport (MQTT) is a machine-to-machine connectivity protocol. It is based on a publish–subscribe model, providing two-way communication through TCP/IP. It was originally developed by IBM for low bandwidth, resource-constrained devices in embedded systems. Because of its low complexity and low power draw, it is a suitable choice for IoT applications. It offers a compact, binary packet payload, which is much simpler than other messaging technologies such as Hypertext Transfer Protocol (HTTP). For this project, we chose the MQTT protocol because it provides a convenient integration with several cloud applications. Nevertheless, other IoT protocols are also available (see [24]).

3. System Design Setup and Diagram

3.1. Layered Functional Diagram

As shown in Figure 1, the overall system can be represented using a CPS master diagram, a layered representation for CPSs [1]. Using systems thinking, this system representation provides useful guidance to represent the architecture of the CPS and support the implementation of a safety and security analysis.

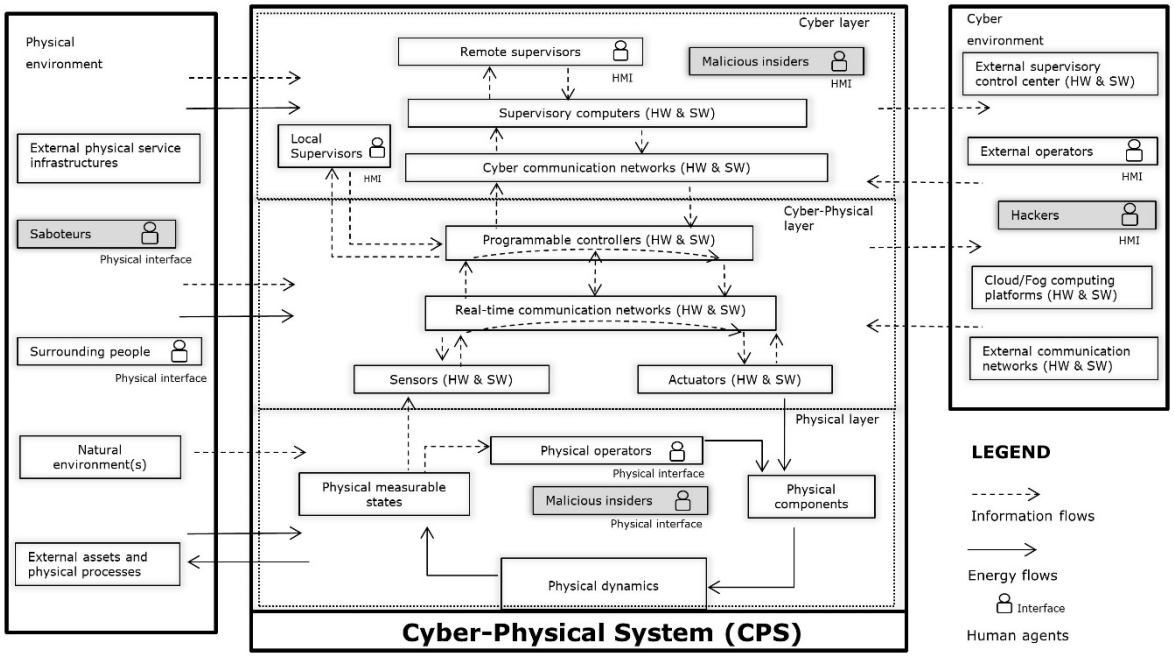

Figure 1. Cyber–physical systems (CPS) master diagram as multi-layered system representation [1].

The CPS master diagram subdivides the system in three layers: cyber, cyber–physical, and physical. The physical layer is composed of parts and processes that are not materialized by computers or digital networks. Instead, they are accomplished by energy transformations between mechanical parts, as well as chemical or other physical processes. Conversely, the cyber layer refers to the computations, communications, and supervisory control processes that are not directly in contact with the physical processes. As an intermediate level, the cyber–physical layer is composed of reactive control functions performed by the embedded system via sensors and actuators. Finally, the CPS as a whole interacts with the cyber and physical environments that are beyond the domain of control of the stakeholders.

Using this multi-layered representation, Figure 2 illustrates the driverless bulldozer system and environments. In the cyber layer, through the dedicated UI, the human operator inserts the routes to be followed by the bulldozer. The information inserted by the operator is transmitted using MQTT via GPRS communications to the microcontroller. Then, the algorithms embedded in the controller process this information, executing the route in the physical layer using sensors as inputs and actuators as outputs. When completing the route segment, or if the sensors detect an obstacle, the bulldozer stops and sends its position and a message to the UI. At the cyber layer, the programmer is also depicted as the developer of the UI and the programmer of the microcontroller.

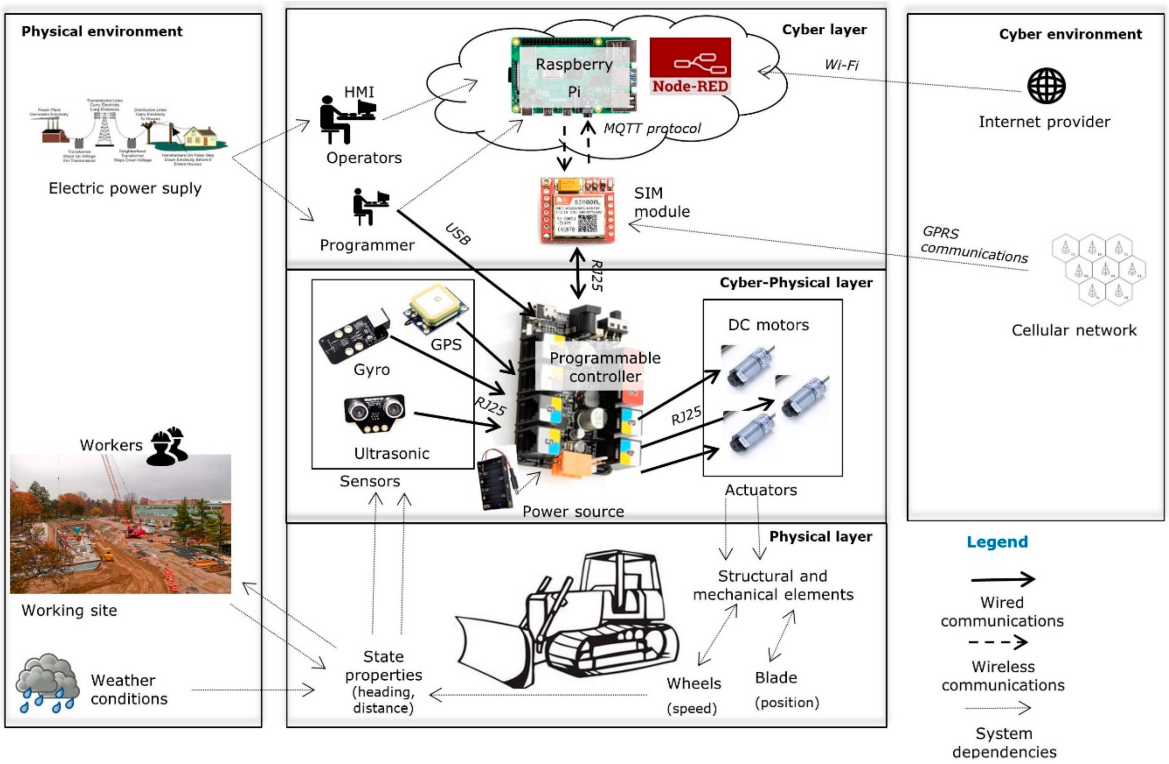

Figure 2. System representation as multi-layered CPS and environments.

The human controller in the remote workstation can access the UI designed in the Node-RED programming tool, which is installed in a Raspberry Pi and accessible via an internet connection. In this way, we can avoid the use of proprietary cloud platforms and achieve an open access and affordable solution that gives the user more control of the data. Finally, a map reports the work progress of driven paths and stores them in ad hoc tables accessible in the UI.

Because the cyber layer of the system communicates using the internet protocol TCP/IP, the CPS requires a combined safety and security analysis that includes generic and targeted cyber threats. In Section 4, we describe how the CPS master diagram assists designers in a preliminary risk assessment for the safer design and allocation of protection barriers.

3.2. Bulldozer Physical Built System

The bulldozer is an original design based on the detecting robot form proposed by the Makeblock Ultimate 2.0 kit [20]. Additionally, a blade mechanism was included to provide the blade functionality of a bulldozer. For this reason, the assembly had to be tailored to provide physical space for the blade mechanism while allowing for a clear space for the ultrasonic sensor to detect obstacles in front of the bulldozer. In Figure 3, the main components of the prototype are illustrated. Note that in this new version in Figure 3b, the GPS module is connected to the microcontroller, providing navigation inputs for the tracking functionality.

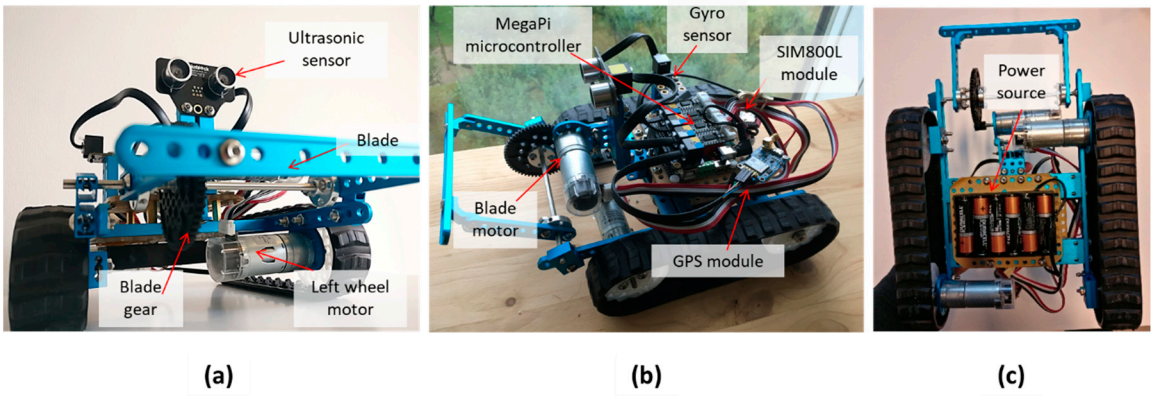

Figure 3. Prototype main views and parts explained (**a**) Front view; (**b**) left side view; (**c**) bottom view.

A set of beams and plates joined by screws compose the chassis. As mechanical moving parts, a configuration of gears and tires transmit the torque from the motors to displace the bulldozer on the ground. Likewise, a gear transmits the rotations from a motor to the blade mechanism to move it up and down.

To avoid latency issues in the critical control functions, the control logic was embedded in the microcontroller on-board the bulldozer. An ultrasonic sensor was placed so that it faces front to detect obstacles ahead when the bulldozer is moving forward. Furthermore, a gyro sensor provides the current heading from its yaw measurement, used to calculate the initial turn. In total, three encoder motors were installed; two of them to move tire gears (one at each side) and one motor to move the blade mechanism. The sensors were connected using serial communications, while the motors were connected through motor drivers.

In this enhanced prototype, a GPS module (GPS Neo 6M) was integrated using serial communications to the microcontroller to ensure the live tracking of the vehicle and to improve the overall security through geofencing functionality. Though global positioning can be achieved purely by triangulation on a cellular network, the accuracy of triangulation is low and GPS technology provides further measurements, such as altitude, heading, and velocity, which are relevant for the developed system.

3.3. Cloud Application and User Interface

As an MQTT broker, the open-source message broker Mosquitto [25] was configured on the microcontroller. Eight different topics were introduced to realize the two-way communication and separate the different information flows. Because the JavaScript Object Notation (JSON) is a popular and well-structured format, all payloads are sent in this format.

As mentioned in the previous section, we used the Node-RED programming tool installed in a Raspberry Pi. As shown in the UI in Figure 4, the operator finds the current status and position of the vehicle in the header of the UI. The status has three states: idle, running and stop. Next to the position widget, three buttons (STOP, RESUME and RESET) were placed to assure on-demand access to basic control functions.

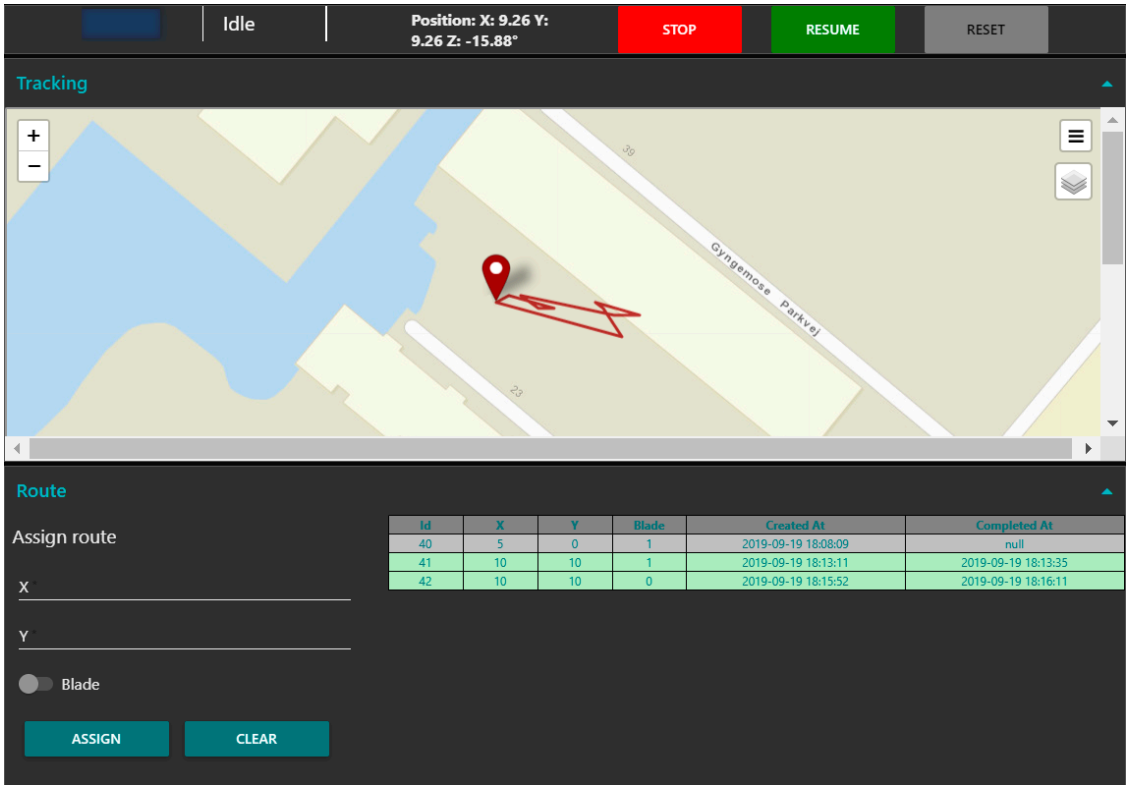

Figure 4. Developed user interface with Global Position System (GPS) tracking designed in cloud platform.

Additionally available in the UI is a geospatial representation of the bulldozer location. This geospatial representation is a set of maps that provides the location of the bulldozer in GPS coordinates. Moreover, the maps are able to depict the routes followed by the bulldozer in the past, providing an overview of the covered territory for monitoring purposes. The last two elements of the user interface are two tables which are not visible in the figure. The first one lists the positions of detected obstacles, while the second one is a history of the bulldozer's position.

The next part of the UI refers to the route segments. First, there is a simple form where the operator can assign routes to the bulldozer by defining the target X and Y coordinates together with a blade position. Next to the form, there is a table listing all the previous routes assigned. In the table, the completed route segments are marked as green and have a completed flag set.

The coded flow diagram for route assignment is illustrated in Figure 5. Similarly, the coded flow for GPS tracking is shown in Figure 6.

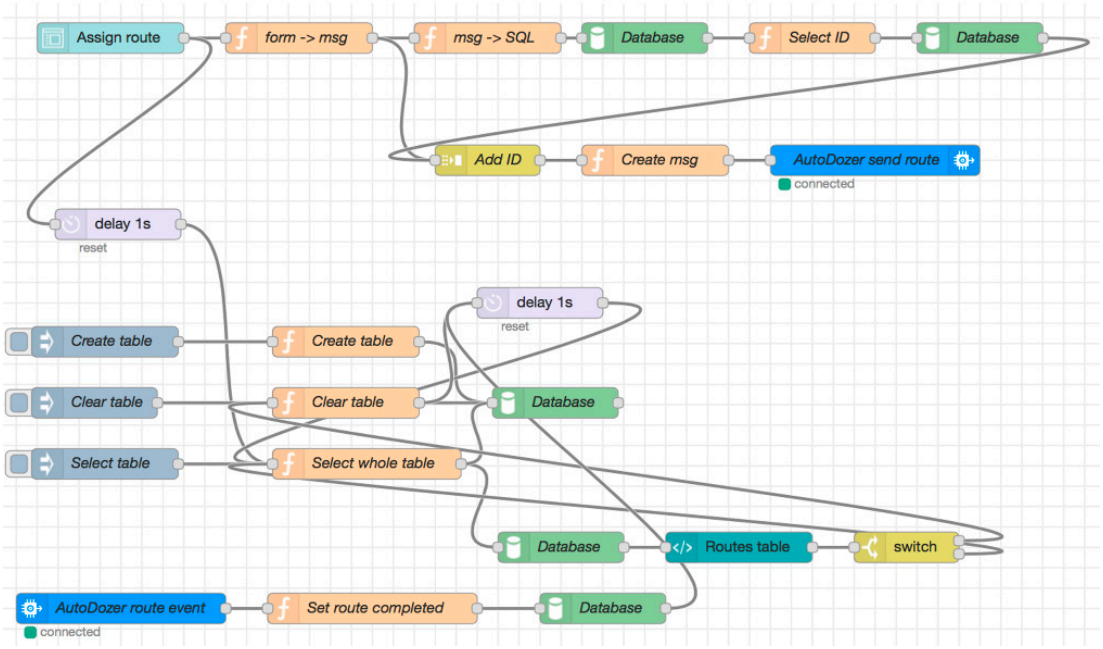

Figure 5. Flow diagram for route assignment in cloud platform.

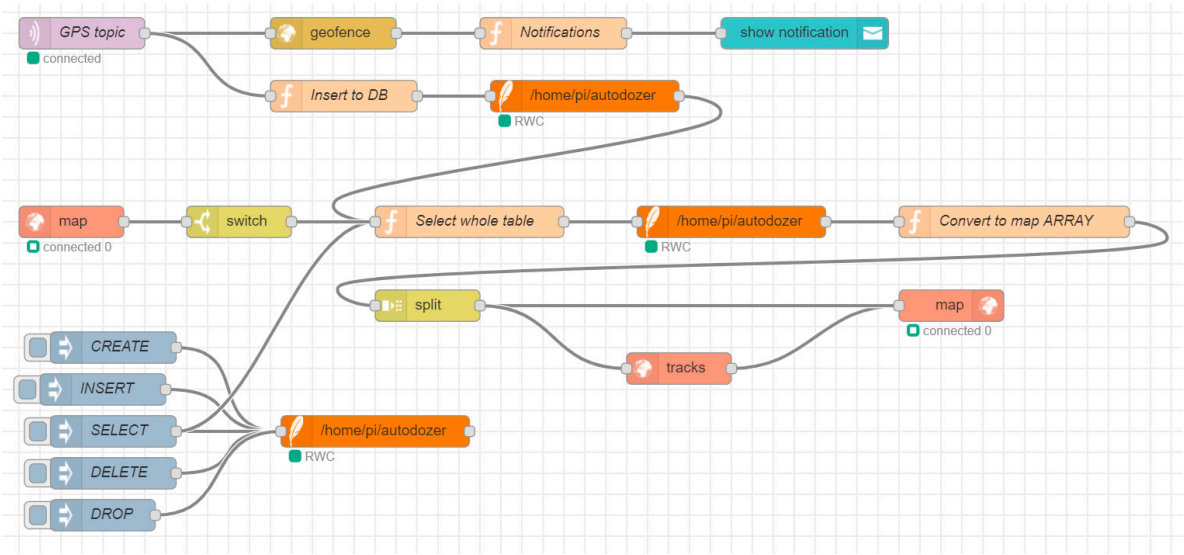

Figure 6. Flow diagram for GPS tracking in cloud platform.

3.4. Conceptual Design of Physical Processes

Beyond the integration of the different communication technologies and the cloud application, we also demonstrated the physical implementation and operation of the system in the small-scale driverless bulldozer. As a conceptual design choice, the route handling was conceived as four sequential control function modes: (1) route assignment, (2) turn while detecting an obstacle, (3) blade to position, and (4) drive forward while detecting an obstacle (see [20]). The cloud application handles each route in a first in first out (FIFO) basis, making the bulldozer perform a sequence of functions for multiple route assignments in a continuous process.

4. Results

We successfully deployed a communication architecture that allows for two-way communications between (a) the UI allocated in a cloud application and (b) the microcontroller on-board the bulldozer

managing the physical commands. The integration of the GPRS cellular network and the MQTT protocol compose this architecture. Despite the use of a cellular network instead of a low power, wide-area network (LPWAN), the use of a cloud application and the MQTT messaging protocol to manage sensors and actuators through a microcontroller provides an IoT-based solution for the design of this CPS. In Table 1, we stress the convenience of using GPRS as a communication technology instead of the competing IoT wide-area network alternatives, which we acknowledged as less powerful and not mature enough to handle this type of safety-critical application. Nevertheless, future developments in Narrowband Internet of Things (NB-IoT) and 5G technologies could become alternatives that are more attractive and provide a faster and more reliable service. In this scenario, only minor revisions would be necessary to adapt the codes and the MQTT topics to a revised communication architecture.

Furthermore, we successfully deployed a dedicated UI in Node-RED for route assignment and on-demand command functions. A database was automatically filled with systematic inputs sent from the microcontroller, reporting assigned routes (completed, or to be completed), obstacle positions, the bulldozer's relative position in the work field, and bulldozer GPS coordinates. Communication between the control unit and sensors, actuators, and modules was successfully established using serial communication. In line with our open-source goals, we have shared our embedded code uploaded to the microcontroller on-board the bulldozer as well as the Node-RED coded flows that designed the UI in the cloud platform and established the communications with the controller on-board the bulldozer [26]. In this way, communities of researchers, developers and users can benefit from this work and expand its functionalities with further developments.

While focusing on the integration of the different communication technologies and the cloud application, we also demonstrated our communication architecture's physical implementation in a small-scale driverless bulldozer. We managed to successfully operate the system in a controlled environment, where we were able to drive route segments and avoid collisions with obstacles.

We encountered some issues in establishing the serial communication between the microcontroller and the GSM module. Nevertheless, these issues were mainly associated with the limitations of the prototype application. The SIM800L is a very sensitive and power-consuming module that requires a proper power supply to keep a robust GPRS connection alive. The module needs 3.4–4.4 V and demands up to 2 A when registering to a network. We managed to provide these conditions through the I/O pins of the microcontroller.

In Table 2, we summarize the results in terms of the functionality of the different functions and technologies integrated in this prototype. Overall, the UI functions were achieved with a high level of reliable execution and timeliness. In contrast, the actual path execution and obstacle detection functions of the bulldozer were achieved with limited confidence levels. This result was expected considering the limitations of the hardware and power source used in this prototype. Nevertheless, we expect these limitations to be solved in real-scale applications, which can benefit from the reliable and scalable properties of the UI and communication architectures described in this work.

Table 2. Detailed report of results of achieved functionality.

Function	Mechanisms	Result
Store and report routes assigned and completed	(1) Database of routes assigned and completed reported in UI (2) Database of obstacles encountered reported in UI	Reliable execution
Geospatial visualization of bulldozer routes	(1) Map visualizations in UI (2) Bulldozer GPS route tracking displayed in UI	Accuracy 2.5 m and close to real-time (<30 s delay)
Human–Computer Interactions	(1) UI with visual and audio notifications (2) UI heading status reports	Reliable execution and real-time (<3 s delay)

Table 2. *Cont.*

Function	Mechanisms	Result
Route assignment	(1) Route assignment fields(2) Route assignment buttons	Reliable execution
Obstacle detection function in bulldozer	(1) Detection sensor (ultrasonic) (2) Stop function in control logic in microcontroller	Limited range Unreliable execution
Route accuracy followed by bulldozer	(1) Encoder motors (2) Control logic in microcontroller	Reliable execution of commands Limited accuracy in turning and driving forward (average 10% path deviations in route points)
Two-way communications UI-microcontroller	(1) GSM module (2) MQTT protocol with eight different topics (3) Integration with Node-red UI	High classification reliability Medium connection reliability (partial disconnections approx. each 20–30 min)

4.1. Discussion of GPS Tracking System

The GPS module was attached via a hardware serial connection to the on-board microcontroller and was programmed with the NeoGPS library [27]. The module had an accuracy of 2.5 m, which might have been low for the prototype scale but would probably be enough for a real-scale bulldozer. Furthermore, the installed sensor provided a reasonable cold and warm start time of 27 s, which also fit our purposes, since the GPS module was always turned on when the engine of the bulldozer was running.

GPS sensors provided measurements using the National Marine Electronics Association (NMEA) sentences. One GPS fix location was built from a sequence of sentences; therefore, the operating system of the bulldozer had to prioritize listening for the NMEA sentences on the hardware serial port. Once a sequence of sentences was provided by the sensor, the GPS had a quiet time in which all the other tasks could be processed.

The MQTT communication was extended with a new topic (evt/gps) to send the measured locations to the cloud application for further processing. Moreover, the Node-RED project was extended with a world map node along with a geofence node. The incoming GPS measurements were saved in the database to provide a historical overview with possible timeline functionality.

A map was placed in the UI and was fed with locations from the database, resulting not only in the UI showing the last valid location but also including the last 10 measurement to have a quick overview of the vehicle movements. Furthermore, every incoming GPS measurement was fed into the geofence node, which checked if the measured location was inside the preset area. If this check resulted in violation, an audio and visual notification was provided in the UI to inform the operator and bring the bulldozer to a safe state. This geofence and alert system enhanced the awareness of remote operators in the control of the bulldozer, providing a more human-centered and robust design of the system to prevent failures and hazardous events in the driverless mode.

4.2. Preliminary Safety and Security Assessment

Recent events have shown the possibility of hackers to access control systems in vehicles and remotely disrupt their operations, leading to hazardous events [28,29]. Using the CPS master diagram representation, we are able to provide preliminary assessment of the safety and security sources of risk that the system should protect against. Using the lessons learned from past events, we mapped the threat actors (hackers) in the cyber environment of the CPS master diagram and the possible attack surfaces that the hackers could target in the system in Figure 7. These cyber threats could evolve into cyber–physical attacks and have repercussions in the physical layer of the system and the physical environment, posing safety risks to people and assets in the working site [30]. This type of assessment

is necessary in early stages of IoT-based CPSs to promote a safer design and human-centered solutions agreed upon by the multidisciplinary design teams [1]. In the following paragraphs, we describe the identified scenarios and some proposed solutions.

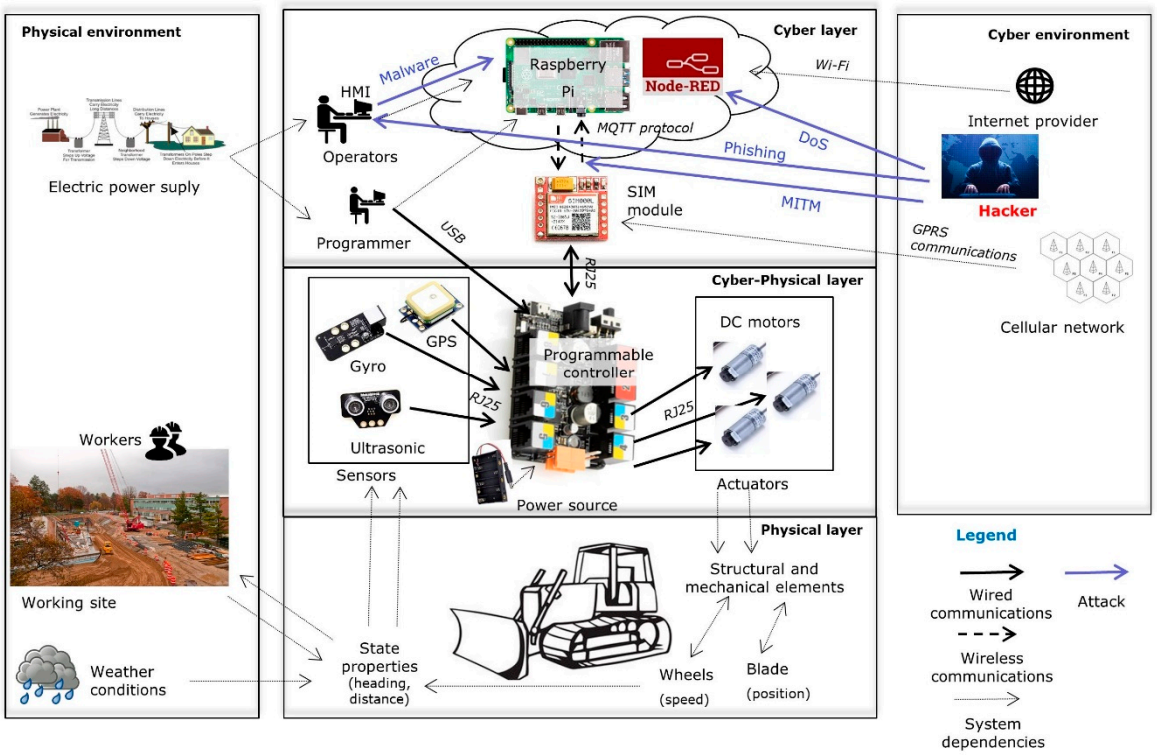

Figure 7. Mapping of threat actors and cyber–physical attack surfaces in CPS master diagram.

4.2.1. Scenario 1: Phishing Attack and Malware Infection

Initially, hackers could target the operator using spear phishing attacks. If successful, this attack could infect the computer workstation in the cyber layer and be used to inject malware into the Raspberry Pi controller connected to it. In this way, the attacker could even gain access to the Node-RED code and modify it at will, disrupting the communications with the microcontroller on the bulldozer of the cyber–physical layer. For this type of attack, mitigation measures include the training of operators against phishing e-mails, disabling connection of potentially infected local drives (e.g., flash drives), intrusion detection systems, among others.

4.2.2. Scenario 2: Man-In-The-Middle (MITM) attack

Even if the attacker is not able to gain local access to the computers, an attack may be targeted via the communication network of the cyber layer. In this scenario, a man-in-the-middle attack would not just conduct eavesdropping on the messages from the cloud platform to the microcontroller on-board the bulldozer. Instead, a hacker with sufficient knowledge of the MQTT protocol credentials and the embedded control algorithm in the microcontroller could compromise the message integrity by intercepting the correct messages and injecting corrupted messages. As a result, the bulldozer functions could be altered towards hazardous conditions, even collisions, if the attacker was able to corrupt the obstacle detection algorithm. For this type of attack, mitigation measures include message encryption, intrusion detection systems in the cyber network, authorization, and authentication barriers.

4.2.3. Scenario 3: Denial of Service (DoS) attack

In terms of cyber–physical security, a less critical attack scenario is a Denial of Service (DoS) attack. In this scenario, a hacker could send superfluous request to the Node-RED application and overload

the system, making it inaccessible to the bulldozer remote operators in the cyber layer. Therefore, the bulldozer could not be remotely controlled, and the work plan could suffer delays. Mitigation measures against these attacks include system redundancy for remote control components and communication channels, as well as authentication and authorization barriers in Node-RED.

4.2.4. Discussion on Preliminary Safety and Security Assessment

We performed a preliminary safety and security assessment to highlight a set of cyber–physical attack mechanisms that remote hackers could use to cause hazardous events. This assessment is different from a traditional cyber security analysis because it goes beyond the scope of ensuring data confidentiality, integrity and availability (CIA). Though the cloud platform contains valuable data that the system users are interested in protecting from CIA violations, the cyber–physical framework in the CPS master diagram highlights how cyber-attacks could evolve into physical deviations in the bulldozer and lead to hazardous consequences to people and valuable assets. This possibility is especially clear in the Scenario 2, where message integrity violations could potentially lead to a dangerous bulldozer collision. A similar case could be made to Scenarios 1 and 3, which compromise integrity and availability goals and could become contributing factors to a subsequent bulldozer accident.

A preliminary safety and security assessment is the first step towards a systematic risk analysis. Based on this preliminary assessment, in future work, we aim at developing a systematic risk analysis method that identifies a comprehensive set of cyber–physical hazard scenarios and prioritizes mitigation measures in terms of a criticality assessment and cost–benefit considerations.

5. Further Developments

In this implementation, we were not aiming to design a prototype with the complex control capabilities of an autonomous vehicle. Instead, we demonstrated that IoT technologies could provide the necessary conditions for a bulldozer to operate in the physical world according to the communication and control commands provided by an operator using the UI. In the following paragraphs, however, we describe potential improvements to the prototype version that could be explored in further work for more realistic applications.

The ultrasonic sensor is an insufficient solution for collision avoidance in real bulldozer use cases, which will require the integration of technologies such as radar, Lidar, or cameras. The sensors and the control logic should incorporate instances to identify obstacle classes and assess the hazardous obstacle collision scenarios from other insignificant obstacles. Moreover, the control logic could be expanded with the possibility to circumvent obstacles with autonomous maneuvers, preferably alerting the remote human controllers when these situations occur.

In the developed GPS tracking system, after startup, the system waits for the first GPS fix and only allows the users to assign routes afterwards. Then, the system prioritizes the GPS sensor and only turns for the other tasks when a fix is received and the GPS is in its quiet time period. This design might entail some issues, since the system cannot be used without adequate coverage, and it also introduces some latency that might be crucial in a system like this. Another solution for processing the continuously incoming sentences could be to use interrupts, which would likely lower the latency. In future developments, a RTK positioning could give accurate GPS coordinate readings to assess the vehicle position in a global reference system, enabling the necessary inputs for feedback control during route execution. Geofencing with automatic situation awareness could also be implemented to avoid accidental or deliberate manipulations outside the working site.

Finally, this application could be extended for a fleet of mobile machineries. This would require additional coordination logic to avoid accidents and implement cooperative functions among the different machineries. Moreover, considering that mobile machinery fleets in real-scale would be safety-critical applications, the need for redundancy in communication and control platforms is recommended.

6. Conclusions

This paper demonstrated the design of a scalable, driverless bulldozer prototype using IoT-based technologies. We illustrated the design process of the overall system and enhanced a preliminary version with new GPS tracking capabilities and remote monitoring functions. We tested the current technologies to operate and supervise the machinery with an improved user interface that provides geospatial information of work progress. We successfully implemented the user interface in a local microcontroller using the Node-RED programming tool and coded flow diagrams, decoupling the cloud application from the proprietary solution used in a previous version of the prototype. Furthermore, we conducted a preliminary safety and security analysis of the prototype system, and we identified the protection measures needed to ensure safe operations in the remote control and semi-autonomous modes. Generalizing from this particular case to the generic design of IoT-based cyber-physical systems, we recommend a preliminary safety and security risk assessment from the early stages of the design process to promote a safe design. Using the CPS master diagram, designers and engineers can identify and protect the security vulnerabilities as well as the human use cases that could potentially lead to hazardous scenarios. This study will serve as a base for future studies of autonomous mobile machineries, enabling an extension of the proposed configuration to semi-autonomous fleets in construction, agricultural, and mining contexts, among others.

Author Contributions: Conceptualization, N.H.C.G. and A.G.M.; methodology, N.H.C.G.; software, A.G.M.; validation, N.H.C.G. and A.G.M.; writing—original draft preparation, N.H.C.G. and A.G.M.; writing—review and editing, N.H.C.G.; supervision, N.H.C.G.

Funding: This research received no external funding.

Acknowledgments: We thank Ying Yan and Martin Nordal Petersen from the Department of Photonics Engineering at the Technical University of Denmark for providing technical support and hardware components to test in our prototype.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Guzman, N.H.C.; Wied, M.; Kozine, I.; Lundteigen, M.A. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Syst. Eng.* **2019**, 1–22. [CrossRef]
2. Rajkumar, R.; Lee, I.L.I.; Sha, L.S.L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010; pp. 731–736.
3. Lee, E.A.; Seshia, S.A. *Introduction to Embedded Systems: A Cyber-Physical Systems Approach*, 2nd ed.; The MIT Press: Cambridge, MA, USA, 2017.
4. Ge, X.; Yang, F.; Han, Q.L. Distributed networked control systems: A brief overview. *Inf. Sci.* **2017**, *380*, 117–131. [CrossRef]
5. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
6. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
7. Monostori, L. Cyber-physical production systems: Roots, expectations and R & D challenges. *Procedia CIRP* **2014**, *17*, 9–13.
8. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4.
9. European Commission. Mobile Machinery. In *Growth: Internal Market, Industry, Entrepreneurship and SMEs*; 2018; Available online: https://ec.europa.eu/growth/sectors/mechanical-engineering/mob_machinery_en (accessed on 5 July 2018).
10. Simonite, T. Mining 24 Hours a Day with Robots. *MIT Technol. Rev.* **2016**. Available online: https://www.technologyreview.com/s/603170/mining-24-hours-a-day-with-robots/ (accessed on 6 July 2018).

11. Underwood, C. The Future of AI in Heavy Industry—Agriculture, Construction, Mining, and Beyond. *Techemergence* **2018**. Available online: https://www.techemergence.com/future-ai-in-heavy-industry/ (accessed on 6 July 2018).
12. Pedersen, S.M.; Fountas, S.; Have, H.; Blackmore, B.S. Agricultural robots—System analysis and economic feasibility. *Precis. Agric.* **2006**, *7*, 295–308. [CrossRef]
13. Stentz, A.; Dima, C.; Wellington, C.; Herman, H.; Stager, D. A System for Semi—Autonomous Tractor Operations. *Auton. Robots* **2002**, *13*, 87–104. [CrossRef]
14. Muoio, D. Google Just Made a Big Move to bring Down the Cost of Self-Driving Cars. *Bus. Insider* **2017**. Available online: http://www.businessinsider.com/googles-waymo-reduces-lidar-cost-90-in-effort-to-scale-self-driving-cars-2017-1?r=US&IR=T&IR=T (accessed on 6 July 2018).
15. Wilson, J.N. Guidance of agricultural vehicles - A historical perspective. *Comput. Electron. Agric.* **2000**, *25*, 3–9. [CrossRef]
16. Mousazadeh, H. A technical review on navigation systems of agricultural autonomous off-road vehicles. *J. Terramech.* **2013**, *50*, 211–232. [CrossRef]
17. Nørremark, M.; Griepentrog, H.W.; Nielsen, J.; Søgaard, H.T. The development and assessment of the accuracy of an autonomous GPS-based system for intra-row mechanical weed control in row crops. *Biosyst. Eng.* **2008**, *101*, 396–410. [CrossRef]
18. Caterpillar Inc. Caterpillar Mining Technology: Autonomous Trucks. 2014. Available online: https://www.youtube.com/watch?v=VkanknGePhc (accessed on 26 April 2018).
19. CNH Industrial. The CNH Industrial Autonomous Tractor Concept (Full Version). 2016. Available online: https://www.youtube.com/watch?v=T7Os5Okf3OQ (accessed on 26 April 2018).
20. Guzman, N.H.C.; Mezovari, A.G.; Yan, Y.; Petersen, M.L. An IoT-Based Prototype of a Driverless Bulldozer. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 291–296.
21. Tardy, I.; Aakvaag, N.; Myhre, B.; Bahr, R. Comparison of Wireless Techniques Applied to Environmental Sensor Monitoring. 2017. Available online: https://www.sintef.no/en/publications/publication/?pubid=CRIStin+1461936: (accessed on 4 November 2019).
22. Vejlgaard, B.; Lauridsen, M.; Nguyen, H.; Kovacs, I.Z.; Mogensen, P.; Sorensen, M. Coverage and Capacity Analysis of Sigfox, LoRa, GPRS, and NB-IoT. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference, Sydney, NSW, Australia, 4–7 June 2017.
23. Wang, H.; Fapojuwo, A.O. A Survey of Enabling Technologies of Low Power and Long Range Machine-to-Machine Communications. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2621–2639. [CrossRef]
24. Al-Fuqaha, A.; Guizani, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
25. Eclipse Foundation. Eclipse Mosquitto^{TM}. An Open Source MQTT Broker. Available online: https://mosquitto.org/ (accessed on 1 August 2018).
26. Guzman, N.H.C.; Mezovari, A. Design of IoT-Based Cyber-Physical Systems: A Driverless Bulldozer Prototype (Open-Source Code). Available online: https://orbit.dtu.dk/en/projects/design-of-iotbased-cyberphysical-systems-a-driverless-bulldozer-prototype-opensource-code(7dc1c4e3-e706-42c4-86e2-589cb4f27631).html (accessed on 31 October 2019).
27. Ublox. NEO-6 U-Blox 6 GPS Modules: Data Sheet. 2011. Available online: https://www.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_(GPS.G6-HW-09005).pdf (accessed on 30 October 2019).
28. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; et al. Experimental security analysis of a modern automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Berkeley/Oakland, CA, USA, 16–19 May 2010; pp. 447–462.

29. Drozhzhin, A. Black Hat USA 2015: The full story of how that Jeep was hacked. *Kaspersky Lab Dly.* **2015**. Available online: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/ (accessed on 10 December 2018).
30. Guzman, N.H.C.; Kufoalor, D.K.M.; Kozine, I.; Lundteigen, M.A. Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel. In Proceedings of the 29th European Safety and Reliability Conference, Lower Saxony, Germany, 22–26 September 2019.