The requirements for using wireless networks with AGV communication in an industry environment

Anna-Lena Kampen
Western Norway University of Applied Sciences
Bergen, Norway
anne-lena.kampen@hvl.no

Marcin Fojcik
Western Norway University of Applied Sciences
Bergen, Norway
marcin.fojcik@hvl.no

Rafal Cupek
Silesian University of Technology
Gliwice, Poland
rafal.cupek@polsl.pl

Jacek Stoj
Silesian University of Technology
Gliwice, Poland
jacek.stoj@polsl.pl

***Abstract*— Ongoing changes in manufacturing, and in particular the growing importance of internal logistics based on Autonomous Guided Vehicles (AGV), makes the use of wireless communication in the industry no longer an option but a necessity. Wireless communication offers including lower installation costs than wired networks, less mechanical wear and tear, and the ability to provide crucial information even with moving AGVs. Robust and reliable wireless communication solutions must accommodate the demanding and changing conditions of the existing industrial environment, such as a variable number of communication elements, possible interference, a large area for which to provide communication, and an organic amount of available battery power. Several types of such communications are available and in use in manufacturing systems. For this reason, AGVs operating in a heterogeneous manufacturing environment must support a different kind of wireless communication and use them in an optimal way for the tasks performed. The aim of this paper is to analyze the different types of sensor networks and the requirements for communication with autonomous vehicles that they fulfill.**

Keywords*— *Autonomous Guided Vehicles (AGV), Machine-to-Machine Communication (M2M), Wireless Network

I. INTRODUCTION

Autonomous guided vehicles (AGVs) are often used in modern manufacturing systems. When AGVs are used, it is necessary to ensure that there is reliable communication with them. There are many challenges to maintaining such communication. One of them is to ensure reliability and sufficiently low latency as well as low power consumption. These requirements should be realized in an industrial environment. There are both fixed elements of the industrial infrastructure in this environment – production stations, gates, security devices – and moving elements – AGV or even people.

These vehicles, autonomously or with a robot (cobot) installed, perform a variety of tasks ranging from unloading raw materials onto production lines, moving materials during the manufacturing process, moving finished goods, loading trailers, etc. To increase the flexibility of using mobile robots, AGVs use wireless solutions to communicate with each other and with the control system. These solutions enable mobile systems to bypass fixed and moving obstacles and interact effectively with the existing infrastructure to maneuver throughout a factory [1].

In industrial environments, implementing wireless communication solutions is difficult. Moving vehicles, which are network elements, create quantitative and qualitative changes in the topology of the network structure. Since factory environments are large areas, sensor network systems should cover the entire area. Additionally, AGVs can enter environments with high levels of electromagnetic interference. Communication requirements also vary from environment to environment, with some involving communication between AGVs. In all of these cases, communication should be reliable, secure, and reasonably fast.

This paper discusses some of the protocols and solutions that are used in sensor networks. Practical communication cases that are encountered in the manufacturing process and possible technical solutions are presented. The outline of the paper is as follows. Chapter 2 presents selected cases of AGV communication in an industrial environment. Chapter 3 presents an attempt to match the requirements of AGVs with the capabilities of sensor networks for communicating in industrial conditions. Chapter 4 discusses and describes to what extent the sensor network meets the requirements. Finally, Chapter 5 summarizes the results and presents the conclusions.

II. USE CASE OF WIRELESS COMMUNICATION WITH AGV

The internal transport systems for routing and supervising AGVs often use navigation systems. However, precise positioning is required at all times, e.g., for AGV that is moving in an environment with other AGVs or other moving elements such as people. AGV should not only avoid obstacles but do it optimally. Avoiding means not only stopping but trying to predict them and find an alternative, safe route. Using all of the possible sensors and communication devices all the time is not very energy efficient. It must be emphasized that a platform has a battery with a limited capacity – one of the goals is to increase the operating time for a platform. There are possibilities of using only the most minor energy-demanding devices. There are two formal aspects for moving vehicles – battery saving and positioning accuracy. In the paper, some cases and requirements for energy and position accuracy are presented. There are different types of communication with AGV [2]:

A. Communication Between AGVs

In the first case, two (or more) vehicles can detect each other's presence and communicate with each other. In such a situation, the vehicles can communicate their presence, detected movements, and possible obstacles to each other in order to optimize their routes. When two AGVs come into contact, their sensors will detect this and stop the vehicles. The next action is to reverse the vehicles and change the routes in order to avoid each other. Avoiding is not always easy, not least because AGVs are designed for forward movement and therefore usually have more sensors at the front of the vehicle. If the AGVs can communicate in good time before they become blocked and each is informed of the other's planned movements, they can change their course to avoid the other vehicle. The same action

Norway, Oslo, June 6-8, 2021
978-1-6654-2854-5/21/$31.00 ©2021 IEEE

also applies to an obstacle that is only visible (for the time being) to one of the vehicles. When another vehicle detects an obstacle, the information about the obstacle is sent other vehicle so that it can prepare to avoid it.

B. Communication Between AGV and Infrastructure

Standard communication. This type of communication can occur with sending/receiving data to and from a Manufacturing Execution System (MES) (orders for transportation tasks, information about AGV) or with the Navigation system (routing). A situation can arise in an unpredictable place and time. The AGV should receive orders and questions about the route all of the time, even when exiting. Typical pieces of information are any route changes, new tasks, or alarms. These messages are typically not extensive and do not have to be time-determined. Moreover, an AGV can send information about the actual task, parameters, possibilities, status, alarms, events, etc. During these regular operations, AGV will contact (cyclically or on-demand) the industry network. This capability should be provided throughout the plant, both indoors and outdoors.

Special situations. These situations can occur when AGV are in defined areas. There are different defined areas, such as permanent production infrastructure and a docking station/production stand. The second situation is different. Once in position, the AGV must perform a specific task. This task may be a precision docking operation in which the AGV must be positioned very precisely at the docking station. During these operations, accurate and reliable communication is crucial. The position data from the AGV's sensors are sent and compared with the position that is received at the station to make the positioning as precise as possible. Depending on the location, other tasks can include opening gates, sending signals to open passageways, or cooperating with signals (e.g., lights). An AGV must send information to a fixed part of the industrial infrastructure, and the system should then check accessibility and safety and open the gate or change the lights. This communication occurs at specific locations and requires the rapid transmission of much information (for docking) and the slow transmission of a small amount of information (for opening gates or changing signals). Communication should cover the entire area of production (indoors and outdoors), should be able to work for a long time on its battery supply, and be active for new orders or information all the time. Most of the time, an AGV needs to send a small amount of data at a relatively low speed. Sometimes (e.g., docking), an AGV needs to send a significant amount of the data at high speed [3].

III. Requirements for the Communication with AGVs

Communication must be well planned according to the requirements of the industrial environment. Time-crucial processes are an innate characteristic of several industrial processes. This time parameter imposes a strict delay requirement for the communication (deterministic). There are some elements that should be considered.

Reliability (fault-tolerance) The goal of reliability is to ensure that an AGV reaches its destination, and in the case of serious loss of communication, an emergency routine must be activated.

Security [4] self-configuration and automation have potential vulnerabilities for attackers to exploit and take control of a system. A harsh environment, unpredictable variations in interference and interruptions, reflections from walls and floors, noise generated from equipment and machinery, etc.

Availability (redundancy required, what happens if crucial data is lost, how to prevent crucial data from being lost). Heterogeneous devices with different energy resources, a CPU, and memory must communicate efficiently. Using different frequency bands, competition between delay-sensitive and delay-insensitive traffic can be prevented. For instance, LoRaWAN can coexist with 802.15.4 without interfering with each other's communication. However, the low data rate of LoRaWAN limits its use to nodes with a limited amount of data to transmit.

The routing paths must be adaptable in order to provide a continuous network connection for the **moving devices**. The MAC layer must also support the dynamic association and disassociation of devices into the local shared media. The goal is that the moving nodes maintain continuous network connection as it leaves and enters new areas of the network topology. For the network layer to support this roaming, redundant paths are probably part of the solutions. Redundancy among the paths, specifically, redundancy among the successor nodes, means that the area in which a node can move while still being within reach of at least one of the current successors is increased. Lost successors must pre-emptively be exchanged by new successors to maintain network connectivity. For the MAC layer to support such roaming, the moving nodes must be continuously included in the schedule of the new areas.

Energy-aware management techniques and routing protocols are crucial for load balancing and increasing the network's overall lifetime. Most sensor networks use a variety of **topologies** with different advantages. The star topology is simple, energy-efficient, and provides predictable performance. The weakness is that the coordinator represents a single point of failure since all data must pass through it. The increased workload means that the energy consumption of the coordinator is high, which causes the battery to dissipate quickly. The mesh topology provides more reliable communication because of redundant paths. Additionally, mesh networks are scalable and have enhanced network flexibility.

IV. Discussion on the Advantages and Disadvantages of Selected Communication Protocols

The communication protocols that are used in industrial networks should be able to handle harsh environments in which interference is likely to occur. The energy consumption must be decreased in order to lengthen the network lifetime. Besides, requirements linked with reliability and bounded delay should be supported, and moving nodes should maintain connectivity while moving. The latter could require the coexistence of protocols. For instance, IEEE802.11 can coexist with an IEEE802.15.4 network so that IEEE802.11 can behave as a backup network in the event that the nodes temporarily lose their connection with the IEEE802.15.4 network when they move out of reach of the current next-hop IEEE802.15.4-nodes. ZigBee are based on IEEE802.15.4 at the lower layers, and

WirelessHART and ISA100.11a are based on IEEE802.15.e at the lower layers [5].

A. IEEE802.15.4

In addition to enabling nodes to enter sleep modes to reduce energy consumption, IEEE802.15.4 supports frequency hopping, TDMA, and various topologies and is, therefore, a good candidate for use in industrial environments. Frequency hopping, in terms of Time Slotted Channel Hopping (TSCH), is used to reduce interference from co-located devices that are using the same frequency band. TSCH was introduced in the IEEE802.15.4e amendment.

The effect of interference was experimentally assessed in [6] [7]. In [6], the tests, which were performed in an office environment, revealed that WiFi interference caused the packet delivery ratio of a significant number of links to drop from 90% to 70%-80%, even when the WiFi network was idle and just emitting the synchronization beacons. In [7], IEEE802.15.4 communication was used in industrial indoor environments, and it was shown that the network performance was strongly dependent on the nature and the peak power of the surrounding electromagnetic interference.

Periodic sleeping is an efficient and frequently used method for reducing energy consumption and lengthening the network lifetime. However, sleeping nodes increase the delays; thus, there is a tradeoff between saving energy and reducing delays. Analytical evaluations using a Markov model in [8] showed that in order to accommodate a certain level of desired latency and throughput, IEEE802.15.4 had to increase its active periods to such an extent that its energy cost was higher compared to TSCH MAC (supported by IEEE802.15.4e). The active periods were increased to accommodate more incoming frames. Conversely, when the latency and throughput requirements were relaxed, 802.15.4 MAC consumed less energy than TSCH.

B. ZigBee

One of the significant advantages of a ZigBee network is the ability of the nodes to save energy and increase the network lifetime. To save energy, the nodes spend a large proportion of the time in the sleep mode. ZigBee is, therefore, especially suitable for applications in which low-power consumption is prioritized over bounded delay [9].

ZigBee falls short of supporting bounded delay because of both the periodic sleep approach [10] and the lack of channel hopping capacity [11] [12]. The latter results in its poor ability to protect against interference, which often is prominent in harsh industrial environments. The result is the loss of data and an increased number of retransmissions, which increase end-to-end delay.

ZigBee can be combined with a more power-hungry technology such as 802.11 WiFi for delay-sensitive data to provide bounded delay for delay-sensitive data while reducing energy consumption for the non-delay-sensitive data. Note that because the transmitting power of WiFi devices is much higher than that of ZigBee devices, ZigBee is more susceptible to coexisting interference. A coexisting ZigBee and WiFi performance that is presented in [13] showed that the impact from WiFi reduces the PDR of ZigBee by up to 51.5% when overlapping channels are used. The experiments presented in [14] showed that whenever the WiFi network was powered on, the transmission of management frames between the APs caused corruption in the received ZigBee. By experimentally measuring the impact of WiFi, Bluetooth, and microwave ovens, [15] reported similar results. Several approaches for improving the performance of ZigBee when it coexists with WiFi are suggested in the literature. For instance, in [16], when the WiFi network detected the presence of ZigBee and prevented any pilot data to from being allocated to any subcarriers where ZigBee operated. The experimental results showed a concurrent ZigBee transmission with a throughput reduction of only 10% to 15%. However, this reduction might not be tolerated when ZigBee transmits mission-crucial data. The ability to supply channel hopping would reduce the impact of any interference. Based on these studies, one could conclude that ZigBee is not very well suited for industrial networks unless it is crucial for reducing energy consumption, and in addition, the delay requirement is relaxed.

C. WirelessHART

For proper communication, both WirelessHART and ISA100.11a support several methods, including channel blacklisting to avoid channels that have a large interference with signals; TDMA technology to minimize the possibility of collisions; channel hopping to reduce interference; redundant routing to enhance reliability; data authentication and integrity to maintain data confidentiality, etc. Both WirelessHART and ISA110.11a can operate in both the star and mesh topologies. The former provides a quick response, which is necessary for time-crucial industrial applications. However, the mesh topology is preferable because it also provides increased robustness of the system, greater tolerance to interferences, and higher reliability. This was confirmed in [17], where extended star and mesh topologies were compared experimentally and evaluated based on their latency and signal level. The network technology that was used was WirelessHART, and the conclusion was that mesh is the preferred topology because it is robust against communication interruptions, and the cost for the spatial expansion is low.

Individual experimental tests of WirelessHART and ISA100.11a when coexisting, first with ZigBee, then with 802.11n, were presented in [18]. The tests were performed in a real industrial environment, and the focus of the tests was the packet loss rate (PLR). When being tested against ZigBee, the WirelessHART and ISA10011a nodes used fifteen channels for channel hopping. As a baseline, the PLR that is caused by the harsh industrial environment was measured before any ZigBee node was activated. The PLR was 0.98% and 1.18% for WirelessHART and ISA100.11a, respectively. Moreover, hopping channels interfered with ZigBee nodes and PLR increased to 1.43% for WirelessHART and 1.62% for ISA100.11a. Thus, the main impact on the PLR was traced back to the harsh environment, although it was expected that the PLR would increase linearly with the number of interfering nodes. The performance of WirelessHART was somewhat better than ISA100.11a because its topology dynamically changed based on factors such as the received signal strength (RSSI) and PLR. The ISA100.11a field devices will maintain the current path as long as the PLR of that path is lower than the threshold.

When Wireless coexists with IEEE802.11n using 15 channels, the PLR of WirelessHART and ISA100.11a are almost equally affected by interference from the WLAN, 3.36% and 3.47%, respectively [18]. The impact from WLAN interference increases with WLAN traffic. ISA100.11a adaptively monitors all of the channels to adaptively switch to the channel with the least interference. Using fewer channels, four instead of fifteen, made WirelessHART more susceptible to interference from the harsh environment. The results showed that dynamic topology management and an increased number of channels to hop between reduced the PLR. The experimental result presented in [6] confirmed the advantage of using channel hopping to reduce the PLR when an IEEE802.15.4 network coexists with WiFi networks. In [6], it was also found that the beaconing activity significantly impacts the link reliability when a WiFi network is idle.

AGVs are likely to experience varying channel conditions when moving to new locations [19]. An experiment with two moving nodes was presented in [6], which showed how a link's packet delivery rate (PDR) evolves. The nodes move along a corridor in an office environment, and IEEE802.15.4 is used for communication. The PDR changes, which range between 0% and 100%, were caused by multipath fading. However, what was positive was that deep fading never occurred on all of the frequencies simultaneously, thus emphasizing the advantage of using channel hopping. It could be expected that for moving nodes, the harsh industrial environment would produce event more PDR variations than office environments.

D. ISA100.11a

ISA100.11a immunity to interference is similar to WirelessHART as was discussed above. The reason is their similar channel hopping algorithms. Because it lacks the ability to support channel hopping, ZigBees' immunity to interference is much lower. In [20], the PER (Packet Error Rate) of ZigBee and ISA100.1 networks were compared in a representative crewed aerospace environment. The examinations showed that high levels of IEEE802.11g interference degraded the success rates of the ZigBee to roughly 65-75%, while that of the ISA100.11a maintained a success rate of more than 99%.

Wireless industrial networks consist of autonomous devices that represent potential vulnerabilities for attackers to exploit in order to take control of a system. In addition, an industrial network is likely to be connected to the Internet. Thus, the security settings of the nodes are crucial. However, it must be remembered that a network consists of heterogeneous devices with different energy, CPU, and memory resources. Most of the security functions in ISA100.11a are optional. Therefore, the load on the processor and energy consumption can be reduced to lengthen the lifetime for devices that do not need strict security functions. This will also reduce the processing time. The disadvantage is that these devices pose a security threat, and as was noted in [21], the industrial infrastructure can be easily targeted and damaged via attacks on the underlying network. By contrast, the security functions are obligatory in WirelessHART, which reduces the threat while increasing the energy consumption and CPU load of all of the devices.

Industrial networks require interconnection with IP networks for remote monitoring, management, data collection and storage. To communicate directly with other IP devices locally or through IP networks, ISA100.11a can use 6LoWPAN at the network and transport layers [22]. To enable direct communication between IEEE802.15.4 networks and IP networks, 6LoWPAN provides header compression and fragmentation to bridge between the different payload sizes that are supported by the IPv6 wireless media [23]. This enables hosts on the Internet to communicate directly with the devices in an ISA100.11a network.

Although multi-hop communication expands the area that can be covered by a network, the price that is paid is increased delays and jitters. The experimental result that was presented for multi-hop communication in [24] showed that increasing the number of hops increased the jitter in the latency, and the suggested reason for this was packet retransmission. The jitter varied even if the quality of the link was good. Increasing the number of hops increased the average delay, which was also pointed out in [25].

E. IEEE802.11

By offering one-hop communication between the nodes and AP, the IEEE802.11 technology supports easy installation and management. In addition, it is relatively long-range compared to other IEEE802.15.4-based technologies, which reduces the amount of management overhead that is required to track the moving nodes.The coexistence of IEEE802.11 Enhanced Distributed Channel Access (EDCA) and Distribution Coordination Function (DCF) was experimentally assessed in [26]. The EDCA mechanism, which was introduced in IEEE802.11e, is used for real-time (RT) traffic, while non-real-time (NRT) traffic uses DCF. The scenario considered three NRT stations whose Basic Service Set (BSS) overlapped the BSS of five RT that were using the same frequency channel.

The RT stations generated periodic traffic with message stream periods (MSPs) of 50ms, 20ms, and 40ms, and generated 20, 50, or 100 packets per second. The NRT stations generated the traffic to occupy 12.5% and 25% of the network load. The requirement for the delay was to be less than the MSPs, and the packet loss rate should be less than 10%. The experiments showed that the EDCA mechanism could not meet the requirements when the medium was shared with the NRT stations. To improve the results, the contention window was tuned, but the loss rate remained higher than 20%. Therefore, the main conclusion was that the EDCA mechanism cannot guarantee the industrial communication requirements unless no other stations are sharing the same medium. It is not likely that all of the possible sources that could emit EMI in the given frequency band can be eliminated in a real industrial environment. As was pointed out in [19], the varying channel conditions that nodes can experience because of location, interference, mobility, etc., is one of the main challenges for supporting QoS in IEEE802.11e.

The simulations that were presented in [25] considering a production site where 90 AGVs periodically communicate to and from five non-overlapping APs using 5 GHz 802.11n showed a delay of less than 3ms. The results indicate that 802.11n might be suitable for an industrial network with AGVs. However, the important effect of other interfering sources was not discussed in the paper, and the question of whether a

seamless handover between non-overlapping APs is feasible was not discussed.

F. Profinet

Some popular industrial Ethernet protocols such as Profinet and EtherCAT can use wireless interfaces [28], [29], but they are applicable with some restrictions. In Profinet, wireless communication can only be used for an RTC1 real-time class data exchange. Wireless is not possible for Profinet IRT, i.e., real-time class RTC3.

The requirement for Profinet with a wireless interface is the operation of a wireless bridge in a transparent mode so that the wireless devices do not modify the MAC addresses in the Profinet datagrams. For mobile clients like AGV, there is an additional requirement for switching between different wireless access points. This is possible in solutions such as Turbo Roaming in wireless devices by MOXA (see: [30]). Moreover, while moving over the factory floor, AGVs do not have to exchange data with all of the Profinet network nodes. This might even be impossible when the access points of their local network are beyond their reach. Therefore, it is required that the communication protocol at the application level has the capability to activate and deactivate some communication tasks according to the current needs. For example, when an AGV reaches a given production stand, the AGV should initialize communication with the network devices on the stand in order to exchange production data. After the operation of the AGV at the stand is finished and the AGV is moving away from it, the AGV should disable communication with the stand. That feature is applicable in Profinet, e.g., using a mechanism called "Docking stations & Docking units". Briefly, it enables the communication tasks with selected devices to be turned on and turned off from the user program that is being used, which is the device that coordinates data exchange in the Profinet network [31].

G. EtherCAT

Like Profinet, wireless communication can also be used together with the EtherCAT Protocols with some restrictions, i.e., only the Ether CAT Automation Protocol EAP datagrams used for communication between EtherCAT master stations can be transmitted wirelessly. The EtherCAT Device Protocol, which is dedicated to the connection of the EtherCAT master with EtherCAT slaves, cannot use a wireless connection because of the way that the datagrams propagate in the network and the on-the-fly datagrams processing that is executed by the slave stations [32]. However, there are attempts to do so in the area [29] where Type 12 PDU or mailbox frames are used to exchange data.

When EAP communication is used, wireless communication is quite feasible. That method of communication is based on the producer-consumer principle of network variables. The EtherCAT master activates or deactivates the production of variables according to current needs. Therefore, the range of communication tasks that can be realized by the EtherCAT master can freely be determined in the user program that is implemented in the master. On the level of the wireless infrastructure, communication using EAP is even simpler than that of the Profinet Protocol. Subscribers can receive the network variables that are sent in the network by using only the variable identifier. Therefore, any changes in the sender's MAC address in the EtherCAT datagrams do not affect communication [33].

TABLE I. COMPARISON OF WIRELESS NETWORKS BASED ON IEEE802.15.4

	ZigBee	***Wireless Hart***	***ISA100.11a***
Based on	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4
Topology	Star, mesh, cluster-tree [8]	Star, mesh [34]	Star, mesh [34]
Channel hopping capability	No, but the frequency of the network might change	Yes Slotted Hopping [34]	
Safety	Symmetric encryption and authentication [34]	All security features are compulsory [35] End-to-end and hop-to-hop – Security Manager [34]	
Energy consumption	Very low [36]	Low	Low
Real time / guaranteed time	No	Yes / no	Yes / no
Access method	TDMA CSMA	TDMA	TDMA / CSMA
Immunity against interference	Poor	Good – TSCH	Good – TSCH
Interoperability toward IP			Easy-through 6LowPAN

TABLE II. COMPARISON OF WIRELESS NETWORKS BASED ON IEEE802.11

	IEEE 802.11	***Profinet RT***	***EtherCAT EAP***
Based on	IEEE 802.11	IEEE 802.11	IEEE 802.11
Topology	Star(a/b/g), (n/ac:supports tree) Mesh not well supported [37]	like IEEE 802.11	like IEEE 802.11
Channel hopping capability	NO	NO	NO
Safety	802.11i RSN Robust Security Network specification	Yes, with Profisafe	Yes, with FSoE (Safety over EtherCAT)
Energy consumption	High or Medium [36]	like IEEE 802.11	like IEEE 802.11
Real time / guaranteed time	no	RTC1 real-time class	producer-consumer principle
Access method	CSMA-CA	CSMA-CA	CSMA-CA
Immunity against interference	Poor – no channel hopping	retransmission	retransmission
Interoperability toward IP	Easy [37]	Easy	Easy

V. SUMMARY

The results of the analysis of wireless communication protocols presented in section IV can be sumarised by key parameters that are crutial for their implementation in the case of comunicvation with AGVs. The comparision of wireless networks based on IEEE802.15.4 is presented in Table 1 and the comparision of networks based on IEEE802.11 is presented in Table 2.

There are some similarities, but there are more differences between them. The protocols that are based on IEEE 802.15.4 use less energy but cannot easily cooperate with other networks. On the other side, protocols based on IEEE 802.11 have much better compatibility but are not so energy efficient during communication. Another parameter, channel hopping availability which is important for the possibility of communication for moving devices, also divides protocols. The environment around moving AGVs can differ. It can be required that AGV should change frequency (channel) to obtain proper communication independently of an industrial environment. This parameter is lacking on protocols based on IEEE802.11. It looks as though in order to have flexibility, it is necessary to use two different types of networks – one to work using the battery for a long period of time and the second for easy and effective operations with other automation systems.

VI. CONCLUSIONS

This paper focus on comparative analyzys of different types of sensor networks and the requirements for communication with autonomous vehicles that they fulfill. Some of different protocols from two groups: based on IEEE802.15.4 and IEEE802.11 have been selected. The protocols were compared due to their suitability for communication with AGVs moving in an industrial environment. Comparison is available both by text description (Section IV) and by tables (Section V). There are set of key parameters presented by the analizys. The summary shows that some protocols are better in energy efficiency and others in compatibility. There is visible that there is no best protocol that can fit all of the requirements. To achieve proper, robust and reliable communication usually, it is necessary to use a combination of these protocols types.

ACKNOWLEDGMENT

The research that led to these results received funding from the Norway Grants 20142021, which the National Centre operates for Research and Development under the project "Automated Guided Vehicles integrated with Collaborative Robots for Smart Industry Perspective" (Project Contract no.: NOR/POLNOR/CoBotAGV/0027/2019 00).

REFERENCES

[1] A. Ziebinski, D. Mrozek, R. Cupek, D. Grzechca, M. Fojcik, M. Drewniak, E. Kyrkjebø, J.C.W. Lin, K. Øvsthus, P. Biernacki, "Challenges associated with sensors and data fusion for AGV-driven smart manufacturing," Lecture Notes in Computer Science book series (LNCS), vol. 12745, pp. 458-470, June 2021.

[2] R. Cupek, M. Drewniak, M. Fojcik, E. Kyrkjebø, J.C.W. Lin, D. Mrozek, K. Øvsthus, A. Ziebinski, "Autonomous Guided Vehicles for Smart Industries–The State-of-the-Art and Research Challenges," Lecture Notes in Computer Science book series (LNCS), vol. 12141, pp. 330-343, 2020.

[3] R. Cupek, Ziebinski A., Fojcik M., "An ontology model for communicating with an autonomous mobile platform," Communications in Computer and Information Science (CCIS), vol. 716, pp. 480-493, April 2017.

[4] J. Q. Li, F.R. Yu, G. Deng,C. Luo, Z. Ming, Q. Yan, "Industrial Internet: A survey on the enabling technologies, applications, and challenges," IEEE Communications Surveys & Tutorials, vol. 19(3), pp. 1504-1526, 2017.

[5] A-L. Kampen, M. Fojcik, R. Cupek , J. Stoj, „Low-level wireless and sensor networks for Industry 4.0 communication – presentation," Communications in Computer and Information Science (CCIS), 2021.

[6] T. Watteyne, C. Adjih, X. Vilajosana, "Lessons learned from large-scale dense IEEE802. 15.4 connectivity traces," IEEE International Conference on Automation Science and Engineering (CASE), pp. 145-150, 2015.

[7] A. Kadri, „ Performance of IEEE 802.15. 4-based wireless sensors in harsh environments," International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 526-530, 2012.

[8] Choudhury, N., Matam, R., Mukherjee, M., and Lloret, J., "A performance-to-cost analysis of IEEE 802.15. 4 MAC with 802.15. 4e MAC modes," IEEE Access, 2020.

[9] Zand, P., Chatterjea, S., Das, K., & Havinga, P., "Wireless industrial monitoring and control networks: The journey so far and the road ahead," Journal of sensor and actuator networks, vol. 1(2), pp. 123-152, 2012.

[10] Marrero, D., Suárez, A., Macías, E., & Mena, V., "Extending the battery life of the ZigBee routers and coordinator by modifying their mode of operation," Sensors, vol. 20(1), pp. 1-22, 2020.

[11] J.Q. Li, F.R. Yu, G. Deng, C. Luo, Z. Ming, Q. Yan, "Industrial Internet: A survey on the enabling technologies, applications, and challenges," IEEE Communications Surveys & Tutorials, vol. 19(3), pp. 1504-1526, 2017.

[12] T. Lennvall, S. Svensson, F. Hekland, "A comparison of WirelessHART and ZigBee for industrial applications," IEEE international workshop on factory communication systems, pp. 85-88, 2008.

[13] X. Wang, K. Yang, "A real-life experimental investigation of cross interference between WiFi and zigbee in indoor environment," IEEE International Conference on Internet of Things (iThings), pp. 598-603, 2017.

[14] Y. Tao, X.Y. Li, C. Bo, „Performance of coexisted wifi and zigbee networks," IEEE 33rd International Conference on Distributed Computing Systems Workshops, pp. 315-320, 2013.

[15] W. Guo, W.M. Healy, M. Zhou, "An experimental study of interference impacts on ZigBee-based wireless communication inside buildings," IEEE International Conference on Mechatronics and Automation, pp. 1982-1987, 2010.

[16] Y. Yan, P. Yang, X. Y. Li, Y. Zhang, "COFFEE: Coexist WiFi for ZigBee networks: A frequency overlay approach," ACM Turing 50th Celebration Conference-China, pp. 1-6, 2017.

[17] M. Kostadinovic, A. Stjepanovic, G.Kuzmic, M. Stojcic, T. Kostadinovic, "Quality Analysis of Data Transferring Through the Process of Modeling WirelessHART Network," 19th International Symposium INFOTEH-JAHORINA (INFOTEH), 2020.

[18] Y. Ding, S.H. Hong, R. Lu, J. Kim, Y.H. Lee, A. Xu, L. Xiaobing, "Experimental investigation of the packet loss rate of wireless industrial networks in real industrial environments," IEEE International Conference on Information and Automation, pp. 1048-1053, 2015.

[19] N. Ramos, D. Panigrahi, S. Dey, „Quality of service provisioning in 802.11 e networks: challenges, approaches, and future directions," IEEE network, vol. 19(4), pp. 14-20, 2005.

[20] R.S. Wagner, R.J. Barton, "Performance comparison of wireless sensor network standard protocols in an aerospace environment: ISA100. 11a and ZigBee Pro," IEEE Aerospace Conference, pp. 1-14, 2012.

[21] M. Cheminod, L. Durante, A. Valenzano, "Review of security issues in industrial networks," IEEE transactions on industrial informatics, vol. 9(1), pp. 277-293, 2012.

[22] T.P. Raptis, A. Passarella, M. Conti, "A Survey on Industrial Internet with ISA100 Wireless," IEEE Access, vol. 8, pp. 157177-157196, 2020.

[23] J.W. Hui, D.E. Culler, "IPv6 in low-power wireless networks," Proceedings of the IEEE, vol. 98(11), pp. 1865-1878, 2010.

[24] W. Ikram, N. Jansson, T. Harvei, N. Aakvaag, I. Halvorsen, S. Petersen, N.F. Thornhill, " Wireless communication in process control loop: Requirements analysis, industry practices and experimental evaluation," IEEE Emerging Technology and Factory Automation (ETFA), pp. 1-8, 2014.

[25] T. Hasegawa, S. Yamamoto, "Design and execution of a "Plant Wide ISA100 Wireless" network for optimization of complex process industries," 54th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), 2015.

[26] J.R.B. Junior, J. Lau, L. de Oliveira Rech, A.S. Morales, R. Moraes, "Experimental Evaluation of the Coexistence of IEEE 802.11 EDCA and

DCF Mechanisms," IEEE Symposium on Computers and Communications (ISCC), 2018.

[27] A. Bujari, A. Corradi, L. Foschini, C.E. Palazzi, „Feasibility of Commodity WiFi for Operations Control in an Autonomous Production Site," IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1-6, 2020.

[28] X. Wu, L. Xie," On the Wireless Extension of PROFINET Networks," IEEE VTS Asia Pac. Wirel. Commun. Symp. APWCS, pp. 1–5, 2019.

[29] X. Wu , L. Xie, "On the Wireless Extension of EtherCAT Networks," IEEE 42nd Conf. Local Comput. Netw. LCN., pp. 235–238, 2017.

[30] C. Chuko, L. Liao, "White Paper: Tips for Deploying Wireless Networks for AS/RS and AGV Systems," 2019.

[31] T. Müller , H.D. Doran, "Protecting PROFINET cyclic real-time traffic: A performance evaluation and verification platform," 14th IEEE Int. Workshop Fact. Commun. Syst. WFCS, pp. 1–4, 2018.

[32] G. Sridevi, A. Saligram, V. Nattarasu, „Establishing EtherCAT Communication between Industrial PC and Variable Frequency Drive," 3rd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. (RTEICT), pp. 1967–1973, 2018.

[33] EtherCAT Automation Protocol, EtherCAT for Plant Automation – standard, (2012) 34. IEEE 802 Working Group, IEEE standard for local and metropolitan area networks—Part 15.4: Low-rate wireless personal area networks (lr-wpans), IEEE Std, 802, 2011.

[34] Q. Wang, J. Jiang, "Comparative examination on architecture and protocol of industrial wireless sensor network standards," IEEE Communications Surveys & Tutorials, 2016.

[35] S. Petersen, S. Carlsen, "WirelessHART versus ISA100. 11a: The format war hits the factory floor," IEEE Industrial Electronics Magazine, vol. 5(4), pp. 23-34, 2011.

[36] A. Willig, K. Matheus, A. Wolisz, "Wireless technology in industrial networks," Proceedings of the IEEE, vol. 93(6), pp. 1130-1151, 2005.

[37] X. Li, D. Li, J. Wan, A.V. Vasilakos, C.F. Lai, S. Wang, "A review of industrial wireless networks in the context of industry 4.0," Wireless net, 2017.