

Idea wykorzystania bezprzewodowej sieci sensorowej i Internetu rzeczy do monitorowania środowiska pracy i ostrzegania pracowników przed zagrożeniami

Fot. ValeryBrozinsky/Bigstockphoto



Występujące w środowisku pracy zagrożenia spowodowane różnego rodzaju czynnikami szkodliwymi są przyczyną powstawania chorób zawodowych. Podejmowanie działań profilaktycznych chroniących pracowników przed nadmiernym narażeniem na czynniki szkodliwe wymaga wiedzy na temat stanu zagrożenia tymi czynnikami w zakładzie pracy. Do monitorowania zagrożeń w środowisku pracy mogą być wykorzystane bezprzewodowe sieci sensorowe.

W artykule przedstawiono podstawowe zagadnienia dotyczące bezprzewodowych sieci sensorowych oraz możliwości realizacji tego rodzaju sieci wykorzystującej rozwiązania z zakresu Internetu rzeczy i przeznaczonej do monitorowania środowiska pracy pod kątem występowania zagrożeń czynnikami szkodliwymi oraz ostrzegania o nich pracowników za pomocą urządzeń noszonych.

Słowa kluczowe: środowisko pracy, czynniki szkodliwe, monitoring, bezprzewodowe sieci sensorowe, Wi-Fi, Bluetooth LE, beacon, Internet rzeczy

The idea of the use of wireless sensor networks and the Internet of things for monitoring the work environment and warning workers about hazards

Hazards caused by various types of factors harmful to health that occur in the work environment are the cause for occupational diseases. Undertaking preventive actions that protect employees against excessive exposure to these factors requires their measurements and assessment of exposure of workers at the workplace. For these purposes wireless sensor networks can be used.

The article presents the basic issues of wireless sensor networks and the possibility of implementing this type of network as well as the Internet of Things to monitor the work environment for the occurrence of hazards caused by harmful factors, and to warn workers about them by means of wearable devices.

Keywords: work environment, harmful factors, monitoring, wireless sensor networks, Wi-Fi, Bluetooth LE, beacon, Internet of Things

Wstęp

W środowisku pracy mogą występować czynniki szkodliwe dla zdrowia pracowników [1]. Według danych GUS w warunkach zagrożenia różnego rodzaju czynnikami środowiska pracy w 2017 r. pracowało w Polsce 262 tys. osób [2]. Zagrożeniem spotykanym najczęściej jest hałas – jest na niego ekspozycja ponad 187 tys. osób. Rzeczywista skala zagrożeń środowiska pracy może być jednak nawet dwukrotnie większa niż podają statystyki GUS, gdyż obejmują one jedynie zakłady pracy zatrudniające 10 lub więcej osób. Szkodliwość dla zdrowia danego czynnika fizycznego (takiego, jak np. hałas, drgania mechaniczne, niesłoneczne promieniowanie elektromagnetyczne, pola elektromagnetyczne, mikroklimat zimny, mikroklimat gorący) [3], chemicznego i pyłowego zależy w znacznym stopniu od wartości natężeń i stężeń tych czynników w środowisku pracy. Z tego względu ustalone są i wprowadzane do stosowania przepisami prawa wartości najwyższych dopuszczalnych stężeń (NDS) i natężeń (NDN) czynników szkodliwych dla zdrowia w środowisku pracy [4, 5]. Praca w narażeniu na czynniki, których stężenie lub natężenie przekracza wartości NDS/NDN może prowadzić do powstawania chorób zawodowych [6], a w skrajnych – do śmierci pracownika.

Obowiązujące przepisy prawa pracy [7-9] zobowiązują pracodawców do dokonywania pomiarów czynników szkodliwych dla zdrowia w środowisku pracy w regularnych odstępach czasu oraz do ograniczania narażenia pracowników na te czynniki do poziomów nieprzekraczających wartości NDS/NDN. Raporty i sprawozdania Państwowej Inspekcji Pracy pokazują jednak, że częstą nieprawidłowością wykazywaną w zakładach pracy jest nieprzeprowadzanie pomiarów lub przeprowadzanie ich nieprawidłowo, bądź za rzadko oraz nieprawidłowa ocena wynikającego z tych zagrożeń ryzyka zawodowego [10]. Często zdarza się też, że pracodawcy i pracownicy, z braku od-

powodniej wiedzy, nie są świadomi występujących w zakładzie pracy zagrożeń. Stężenie lub natężenie czynników szkodliwych może również ulegać zmianie np. w wyniku zmian parametrów procesu pracy, bądź zużywania się maszyn i narzędzi, powodując zwiększenie poziomu ryzyka dla pracowników. W takich przypadkach pracownicy mogą być narażeni na działanie czynnika szkodliwego środowiska pracy przekraczającego wartości NDS/NDN. Wykrycie zagrożenia oraz szybka i skuteczna reakcja, mająca na celu ograniczenie jego wpływu na zdrowie pracownika, jest w takich przypadkach możliwa przy założeniu ciągłego monitoringu parametrów środowiska pracy.

Celem artykułu jest przedstawienie możliwości wykorzystania bezprzewodowych sieci sensorowych i Internetu rzeczy do monitorowania środowiska pracy i ostrzegania pracowników przed zagrożeniami na przykładzie sieci sensorowej opracowywanej w Centralnym Instytucie Ochrony Pracy – Państwowym Instytucie Badawczym.

Sieć sensorowa i Internet rzeczy

Obecny postęp techniki, w szczególności w zakresie technik informacyjnych, automatyki, sztucznej inteligencji, komunikacji bezprzewodowej, czujników wielkości fizycznych i chemicznych, układów przetwarzania cyfrowego sygnałów oraz układów zasilania, umożliwił rozwój i coraz powszechniejsze zastosowanie w różnych dziedzinach życia tzw. bezprzewodowych sieci sensorowych (ang. *Wireless Sensor Network – WSN*) [11-13]. Bezprzewodową sieć sensorową można zdefiniować jako grupę specjalizowanych sensorów oraz układów (urządzeń) wykonawczych wraz z infrastrukturą do komunikacji bezprzewodowej, przeznaczonych do monitorowania i sterowania stanem układów fizycznych lub środowiska w różnych lokalizacjach, tworzących sieć, przez którą przekazywane są dane i polecenia sterujące.

Urządzenia tworzące bezprzewodową sieć sensorową nazywane są węzłami sieci i mogą pełnić w niej różne funkcje. Obok wspomnianych już sensorów i układów wykonawczych mogą być to routery i bramy sieciowe. Każdy węzeł sieci połączony jest z co najmniej jednym innym węzłem. Konstrukcja węzła obejmuje najczęściej odpowiedni przetwornik, mikrokontroler i układ radiowy. Oprogramowanie mikrokontrolera węzła może realizować różnego rodzaju algorytmy obliczeniowe oraz procesy decyzyjne. Dzięki temu układy sensorowe, jak i cała bezprzewodowa sieć sensorowa, mogą reagować na zmieniające się parametry otoczenia i dostosowywać swoje działanie do tych parametrów. Z tego względu określa się je mianem inteligentnych (od angielskiego *smart*).

Kolejnym krokiem rozwoju bezprzewodowych sieci sensorowych było ich połączenie z siecią Internet. Połączenie takie otwiera szereg nowych możliwości funkcjonowania bezprzewodowych sieci sensorowych i wynikających z nich korzyści. Użytkownik sieci może mieć do niej dostęp (tzn. pobierać dane, nadzorować, wydawać polecenia) z dowolnego miejsca z dostępem do Internetu. Bezprzewodowa sieć sensorowa

może również przysyłać dane z układów sensorowych do tzw. chmury obliczeniowej w celu ich przetwarzania (jeżeli nie dysponuje odpowiednimi zasobami np. mocą obliczeniową, pamięcią). Co najważniejsze, dzięki połączeniu z siecią Internet urządzenia zawarte w bezprzewodowej sieci sensorowej mogą się bezpośrednio komunikować z innymi urządzeniami podłączonymi do Internetu (bez udziału człowieka), przysyłając pomiędzy sobą dane lub polecenia. Bezpośrednia komunikacja pomiędzy urządzeniami określana jest jako M2M (ang. *machine-to-machine*) lub rzadziej T2T (ang. *thing-to-thing*). Połączenie bezprzewodowych sieci sensorowych z Internetem stało się początkiem Internetu rzeczy (ang. *Internet of Things, IoT*), czyli Internetu, w którym maszyny komunikują się z maszynami [14-20]. Określenie to zostało po raz pierwszy użyte w 1999 r. przez Kevina Ashtona w prezentacji przeznaczony dla firmy Procter & Gamble [14]. Rozwój bezprzewodowych sieci sensorowych oraz IoT i ich coraz powszechniejsze zastosowanie w przemyśle doprowadziły do zmian nazwanych czwartą rewolucją przemysłową lub przemysłem 4.0 (termin po raz pierwszy został użyty w 2011 r. [21] w strategii rządu Niemiec dotyczących nowych technologii), [22, 23]. W przemyśle 4.0 następuje zintegrowanie systemów produkcyjnych oraz łączenie się inteligentnych systemów, maszyn i urządzeń w sieci odwzorowujące w pewnym stopniu świat realny i umożliwiające systemom realizację zdecentralizowanych procesów decyzyjnych.

Cechą charakterystyczną przemysłu 4.0 jest coraz większe przenikanie się świata ludzi i inteligentnych maszyn, wymieniających ze sobą informacje w procesie produkcji dzięki wzajemnemu przenikaniu się Internetu, Internetu rzeczy, stosowaniu odpowiednich rozwiązań z zakresu technologii informacyjnej czy też coraz powszechniejszych urządzeń nasobnych (inaczej: ubieralnych, ang. *wearables*; są to ubrania oraz akcesoria noszone przez człowieka, zawierające układ komputerowy oraz zaawansowane technologie elektroniczne i mogące komunikować się pomiędzy sobą). Pozwala to stworzyć zoptimalizowane pod względem wykorzystania dostępnych zasobów środowisko produkcyjne, mogące dynamicznie reagować na zmieniające się potrzeby rynku. Obecnie bezprzewodowe sieci sensorowe oraz IoT znajdują zastosowanie między innymi w [13, 15, 16, 17, 18, 24, 25, 26, 27]:

- automatyzacji i monitoringu procesów przemysłowych
- planowaniu, optymalizacji i nadzorowaniu przepływu towarów w logistyce i transporcie
- sterowaniu oświetleniem, zarządzaniu ruchem i miejscami parkingowymi w miastach (tzw. inteligentne miasta – ang. *smart cities*)
- zarządzaniu środowiskiem w budynkach przemysłowych i mieszkalnych (m.in. sterowania oświetleniem, temperaturą, wentylacją) oraz automatyzacji budynków (m.in. tzw. inteligentne domy – ang. *smart homes*)

- monitorowaniu stanu zdrowia pacjenta w czasie rzeczywistym, diagnostyce schorzeń, dozowaniu leków (telemedycyna i in.)
- zdalnym nadzorowaniu pojazdów oraz ich stanu technicznego

- monitorowaniu stanu środowiska
- monitorowaniu i zarządzaniu hodowlą i uprawami w rolnictwie.

Konstruowanie bezprzewodowej sieci sensorowej wiąże się z wykorzystaniem w tej sieci co najmniej jednego z istniejących standardów komunikacji bezprzewodowej do przesyłania danych pomiędzy węzłami sieci. Do najpowszechniej stosowanych w sieciach sensorowych zalicza się standardy:

- Wi-Fi, zestaw standardów będący podstawą współczesnych lokalnych bezprzewodowych sieci komputerowych, opisanych w specyfikacjach IEEE 802.11a/b/g/n, cechujący się dużą przepustowością danych [13]¹

- Bluetooth i Bluetooth Low Energy (Bluetooth LE, Bluetooth Smart) – standard opisany w specyfikacji IEEE 802.15.1, obecnie rozwijany przez Bluetooth Special Interest Group (SIG), wykorzystywany głównie do komunikacji na bliskie dystanse²

- ZigBee, bazujący na standardzie IEEE 802.15.4, do tworzenia sieci bezprzewodowych o niewielkim poborze energii oraz niedużej przepustowości, obecnie rozwijany przez Zigbee Alliance³.

Zastosowanie sieci sensorowej i IoT do monitorowania środowiska pracy i ostrzegania pracowników o zagrożeniach

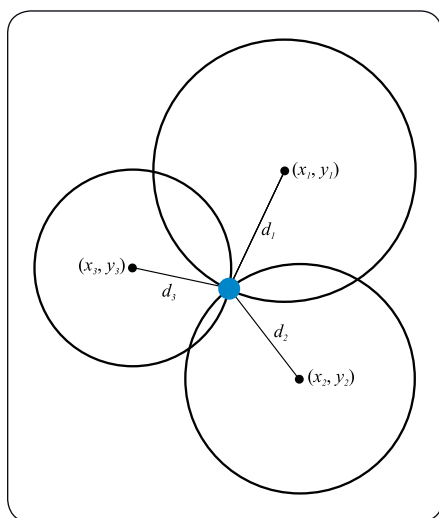
Rozwiązania leżące u podstaw przemysłu 4.0 takie jak bezprzewodowe sieci sensorowe, IoT czy urządzenia nasobne, mogą i powinny przyczynić się do kształtowania bezpiecznego i przyjaznego dla człowieka środowiska pracy. Internet rzeczy, w którym urządzenia wyposażone w opcje komunikacji bezprzewodowej oraz elementy sztucznej inteligencji, mogą komunikować się pomiędzy sobą w celu realizacji odpowiednich zadań, może być zastosowany również do tworzenia sieci sensorowych, monitorujących zagrożenia w środowisku pracy. W sposób inteligentny wpływają one na zachowania i działania pracowników i pracodawców, ułatwiając unikanie tych zagrożeń.

Sieć taka powinna składać się z autonomicznych urządzeń pomiarowych (sensorów), pozwalających na monitorowanie zagrożeń istniejących w środowisku pracy oraz noszonych przez pracowników urządzeń nasobnych, przekazujących im informację o występujących w danym miejscu zagrożeniach. Dzięki temu pracownicy będą mogli modyfikować i dostosowywać swoje zachowanie do panujących warunków środowiska pracy, np. unikać stref zagrożenia czy trafniej dobierać środki ochrony indywidualnej. Bieżący monitoring środowiska pracy umożliwi

¹ <https://www.wi-fi.org/>

² <https://www.bluetooth.com/>

³ <https://www.zigbee.org/>



Rys. 1. Wyznaczanie położenia obiektu metodą triangulacji (obiekt lokalizowany – kolor niebieski, (x_i, y_i) – współrzędne położenia nadajników, d_i – odległość nadajnik – odbiornik)

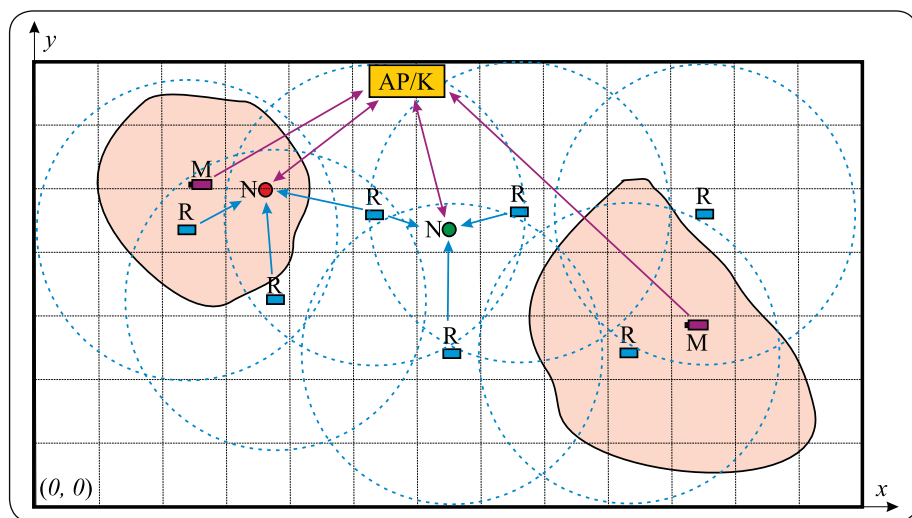
Fig. 1. Determination of the position of the object using the triangulation (localized object – blue color, (x_i, y_i) – coordinates of the transmitters, d_i – distance transmitter – receiver)

również szybką reakcją służb bhp na zmianę zagrożenia lub pojawiający się nowy jego typ.

Sieć sensorowa opracowana na potrzeby monitoringu środowiska pracy i oceny pracowników przed zagrożeniami powinna nie tylko dokonywać pomiaru i oceny zagrożeń występujących w tym środowisku, ale również mieć możliwości lokalizacji położenia pracowników w odniesieniu do położenia stref zagrożenia (rozumianych jako obszary przedsiębiorstwa, w których występują zagrożenia przekraczające wartości NDN/NDŚ). Jest to podyktowane potrzebą ostrzegania pracownika o zagrożeniu w momencie znalezienia się w strefie tego zagrożenia.

Lokalizacja pracownika w obszarze zakładu pracy może być zrealizowana przez urządzenia radiowe (komunikacji bezprzewodowej), wchodzące w skład sieci sensorowej. Do oceny odległości pomiędzy odbiornikiem a nadajnikiem sygnału radiowego można wykorzystać fakt, że moc sygnału odbieranego jest odwrotnie proporcjonalna do odległości pomiędzy odbiornikiem a nadajnikiem. Przy stałej mocy nadajnika można zatem, na podstawie pomiaru mocy sygnału odbieranego, oszacować odległość pomiędzy tymi urządzeniami. W sieciach komunikacji bezprzewodowej moc sygnału odbieranego ma istotny wpływ na proces nawiązywania połączenia pomiędzy urządzeniami oraz na jakość transmisji danych.

W fizycznej warstwie protokołów sieciowych wprowadzono zatem możliwość pomiaru mocy sygnału odbieranego. W standardzie IEEE 802.11, na którym bazuje technologia Wi-Fi, zdefiniowano pojęcia wskaźnika mocy sygnału odbieranego RSSI (ang. *Received Signal Strength Indicator*). Wskaźnik RSSI wprowadzono również w innych standardach bezprzewodowej transmisji danych, takich jak Bluetooth. Wartość RSSI informuje zatem pośrednio o odległości pomiędzy nadajnikiem a odbiornikiem. Przy pomocy metody triangulacji możliwe jest



Rys. 2. Struktura i zasada działania sieci sensorowej do monitorowania środowiska pracy i ostrzegania o zagrożeniach (M – układ pomiarowy – nadajnik, N – urządzenie nasobne, R – beacon, AP/K – punkt dostępowy + komputer, strzałki niebieskie – kierunek transmisji danych Bluetooth LE, strzałki fioletowe – kierunki transmisji danych Wi-Fi, x, y – osie układu współrzędnych, kolor różowy – strefa zagrożenia, linie czarne przerywane – siatka układu współrzędnych, niebieskie okręgi – zasięg transmisji radiowej beacona)

Fig. 2. Structure and principle of operation of sensor network to monitor the work environment, and to warn about hazards (M – measuring device – transmitter, N – wearable device, R – beacon, AP / K – access point and computer, blue arrows – direction of data transmission using Bluetooth LE, violet arrows – direction of data transmission using Wi-Fi, x, y – coordinate system axes, pink color – danger zone, black dashed lines – coordinate system grid, blue dashed circles – radio transmission range of beacon)

określenie położenia odbiornika w zdefiniowanym układzie współrzędnych.

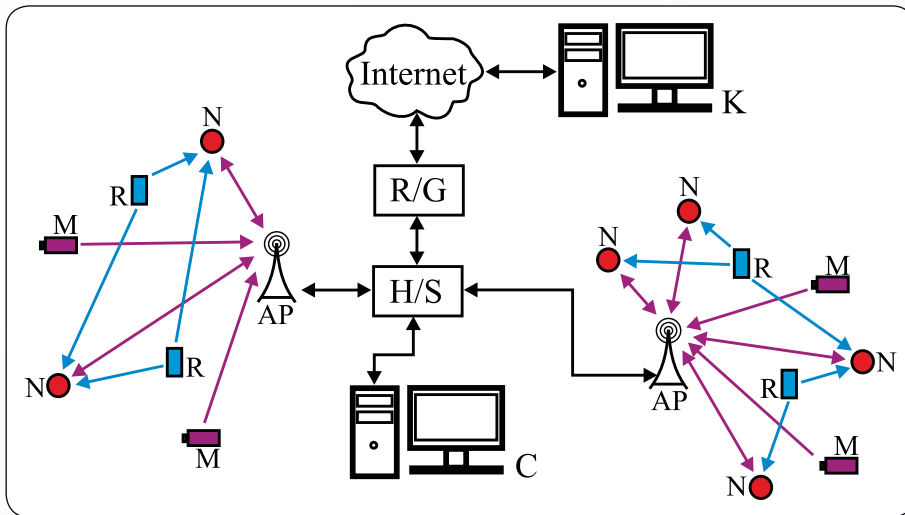
Zasadę wyznaczania położenia obiektów z wykorzystaniem metody triangulacji przedstawiono na rys. 1. Metoda ta wymaga rozmieszczenia w nadzorowanej przestrzeni co najmniej 3 nadajników sygnału. Znając współrzędne x i y położenia nadajników oraz odległości d lokalizowanego obiektu od poszczególnych nadajników, wyznaczone na podstawie pomiaru RSSI, możemy na podstawie odpowiednich zależności geometrycznych wyznaczyć współrzędne położenia lokalizowanego obiektu. Na dokładność oceny położenia pracownika będzie miała oczywiście wpływ dokładność oceny odległości od poszczególnych nadajników. Tego rodzaju metody oceny odległości oraz położenia obiektów (w tym osób) są coraz powszechniej stosowane w praktyce. Dużą popularność zyskały w tym zakresie rozwiązania bazujące na tzw. beaconach⁴ [28], czyli niewielkich nadajnikach radiowych pracujących w standardzie Bluetooth⁵. Komercyjne systemy lokalizacji wykorzystujące beacony są dostępne na rynku⁶. Sieć sensorowa służąca do monitoringu środowiska pracy i ostrzegania pracowników o zagrożeniach powinna wykorzystywać zatem tego rodzaju urządzenia do lokalizacji urządzenia nasobnego (i tym samym noszącego je pracownika) w obszarze zakładu pracy.

⁴ Bluetooth beacon – termin ten nie ma obecnie powszechnie przyjętego polskiego odpowiednika. W języku angielskim beacon może oznaczać m.in. latarnię morską, radiolaternię lub boję sygnalizacyjną. W literaturze spotykane są dwa ostatnie określenia (rzadko), jak również spolszczona wersja słowa beacon.

⁵ https://en.wikipedia.org/wiki/Bluetooth_low_energy_beacon

⁶ <https://estimote.com/products/>

Strukturę i zasadę działania opracowywanej w CIOP-PIB sieci sensorowej, która umożliwi monitoring środowiska pracy i ostrzeganie pracowników przed zagrożeniami, przedstawiono na rys. 2. Obszar przedsiębiorstwa, w którym funkcjonuje rozważana sieć sensorowa, wpisany jest w pewien arbitralnie określony układ współrzędnych. Należące do sieci układy pomiarowe (ozn. M na rys. 2.), oraz beacony (R) są rozmieszczone w punktach, których współrzędne w przyjętym układzie współrzędnych są zgromadzone w bazie danych centrali sieci (jest to komputer gromadzący i przetwarzający dane pomiarowe – na rys. 2. przedstawiony jest symbolicznie jako AP/K). W tym samym miejscu są również zgromadzone współrzędne punktów określających granicę stref zagrożenia. Funkcjonujący w sieci układ nasobny pobiera dane dotyczące mocy sygnału (RSSI) od najbliższych beaconów, a następnie przekazuje je do centrali sieci. Centrala na podstawie przesłanych danych (zawierających numery identyfikacyjne beaconów i wartości RSSI) oraz danych o lokalizacji beaconów, wyznacza metodą triangulacji (lub pokrewnymi) położenie urządzenia nasobnego (pracownika) w układzie współrzędnych. Następnie centrala sieci, na podstawie posiadanych danych, dotyczących stref zagrożenia, ocenia położenie urządzenia nasobnego względem stref zagrożenia. Jeżeli urządzenie nasobne znajduje się w strefie zagrożenia, centrala wysyła do niego odpowiedni komunikat o zagrożeniu. Standardem transmisji bezprzewodowej wykorzystywanym przez beacony i urządzenia nasobne do lokalizacji położenia pracownika jest Bluetooth LE. Do transmisji danych pomiarowych w sieciach sensorowych często wykorzystywany jest standard ZigBee



Rys. 3. Przykładowa struktura sieci sensorowej (M – układ pomiarowy, N – urządzenie nasobne, R – beacon, AP – punkt dostępowy, C – centrala sieci (komputer), H/S – koncentrator lub przełącznik, R/G – router i brama sieciowa, K – komputer łączy się z siecią poprzez Internet (odczyt danych, nadzór), strzałki fioletowe – połączenia bezprzewodowe Wi-Fi, strzałki niebieskie – połączenia bezprzewodowe Bluetooth, strzałki czarne – połączenia ethernetowe)

Fig. 3. The example of sensor network structure (M – measuring device, N – wearable device, R – beacon, AP – access point, C – network main unit (computer), H/S – ethernet hub or switch, R/G – router and gateway, K – computer connected to the network via the Internet (data reading, supervision), violet arrows – Wi-Fi connections, blue arrows – Bluetooth LE connections, black arrows – Ethernet connections)

[29], jednak w przypadku opracowywanego rozwiązania transmisję danych pomiarowych z układów sensorowych oraz danych pomiędzy urządzeniami nasobnymi a centralą sieci zaprojektowano w standardzie Wi-Fi. Wynika to m.in. z dostępności na rynku modułów radiowych pracujących w określonym standardzie (w tym modułów mających jednocześnie wbudowaną obsługę standardów Bluetooth LE oraz Wi-Fi), czy możliwości łatwiejszego wykorzystania protokołu internetowego (IP) i połączenia z istniejącą infrastrukturą sieci komputerowej przedsiębiorstwa.

Schemat sieci sensorowej z uwzględnieniem elementów infrastruktury sieciowej zapewniających komunikację sieci sensorowej z centralą systemu i Internetem przedstawiono na rys. 3. W opisanej sieci sensorowej układy pomiarowe i urządzenia nasobne komunikują się z punktem dostępowym sieci Wi-Fi (ozn. AP na rys. 3.). Dzięki bezpośredniemu wykorzystaniu w sieci Wi-Fi protokołu internetowego (IP) będącego podstawą funkcjonowania Internetu, dane z punktu dostępowego poprzez łącze ethernetowe (kablowe), z wykorzystaniem takich urządzeń sieciowych jak koncentrator lub przełącznik (H/S) oraz router i brama sieciowa (R/G), mogą być przesyłane do komputera będącego centralą sieci (C) i do innych komputerów (K) podłączonych do Internetu (np. w celu zdalnego nadzoru środowiska pracy przez osoby odpowiedzialne).

Podsumowanie

Bezprzewodowe sieci sensorowe, w tym wykorzystujące rozwiązania z obszaru Internetu rzeczy, mogą stanowić znakomite narzędzie do monitorowania środowiska pracy i ostrzegania pracowników przed zagrożeniami. Tego rodzaju monitoring umożliwi niezwłoczne reagowanie na pojawiające się zagrożenia lub zmiany natężeń

już istniejących zagrożeń. Dane na temat zagrożeń występujących w zakładzie pracy zagrożeń, zbierane w wielu jego punktach i w dłuższych odcinkach czasu, umożliwią również odpowiednie projektowanie procesów pracy czy działań profilaktycznych, ograniczających narażenie pracowników na czynniki szkodliwe środowiska pracy. Dostępne obecnie technologie elektroniczne i informatyczne w pełni umożliwiają realizację tego rodzaju sieci sensorowej.

W trakcie dalszych prac oraz w celu rozwijania tytułowej idei, konieczne jest jednak opracowanie odpowiednich układów pomiarowych i urządzeń nasobnych uwzględniających specyfikę przewidywanego zastosowania.

BIBLIOGRAFIA

- [1] Koradecka D. (red.) *Bezpieczeństwo i higiena pracy*. CIOP-PIB, Warszawa, 2008
- [2] *Warunki pracy w 2017 r.*, Główny Urząd Statystyczny, Warszawa, 2018
- [3] *Serwis internetowy „Bezpieczniej”*. <http://www.ciop.pl/bezpieczniej>
- [4] Augustyńska D., Pośniak M. *Czynniki szkodliwe w środowisku pracy. Wartości dopuszczalne*. Międzyresortowa Komisja ds. Najwyższych Dopuszczalnych Stężeń i Natężeń Czynników Szkodliwych dla Zdrowia w Środowisku Pracy, CIOP-PIB, 2016
- [5] Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 12 czerwca 2018 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy, Dz.U. 2018 poz. 1286
- [6] Instytut Medycyny Pracy im. prof. dra med. Jerzego Nofera *Dane o zapadalności na choroby zawodowe* http://www.imp.lodz.pl/home_pl/o_inytucie/reg_and_databases/work_dissises1/dane_o_zapadalnosci/
- [7] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, Dz.U. 1974 Nr 24 poz. 141, tekst jednolity Dz.U. 2016 poz. 1666
- [8] Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy, Dz.U. 1997 Nr 129 poz. 844, tekst jednolity Dz.U. 2003 nr 169 poz. 1650
- [9] Rozporządzenie Ministra Zdrowia z dnia 2 lutego 2011 r. w sprawie badań i pomiarów czynników szkodliwych dla zdrowia w środowisku pracy, Dz.U. 2011 Nr 33 poz. 166
- [10] *Sprawozdanie z działalności Państwowej Inspekcji Pracy w 2016 roku*. Państwowa Inspekcja Pracy, Warszawa 2017 r.
- [11] Benini L., Farrella E., Guiducci C.: *Wireless sensor networks: Enabling technology for ambient intelligence*. *Microelectron. J.* 37(12), 1639–1649 (2006)
- [12] Yang S.H., Cao Y. *Networked control systems and wireless sensor networks: Theories and applications*. *Int. J. Syst. Sci.* 2008, 39, 11:1041-1044
- [13] Yang S.-H. *Wireless Sensor Networks – Principles, Design and Applications*. Springer, London 2014
- [14] Ashton K. *That ‘Internet of Things’ Thing*. “RFID Journal”, <http://www.rfidjournal.com/articles/view?4986>
- [15] Gubbi J., Buyya R., Marusic S., Palaniswami M. *Internet of Things (IoT): A vision, architectural elements and future directions*. “Future Generation Computer Systems” 2013, 29:1645-1660
- [16] Miorandi D., Sicari S., De Pellegrini F., Chlamtac I. *Internet of things: Vision, applications and research challenges*. “Ad Hoc Networks” 2012, 10:1497-1516
- [17] Galio S., Lo Re G. (eds) *Advances onto the Internet of Things. How Ontologies Make the Internet of Things Meaningful*. Springer 2014
- [18] Karimi K., Atkinson G. *What the Internet of Things (IoT) needs to become reality*. White Paper freescale.com/arm.com, <https://www.nxp.com/docs/en/white-paper/INTOTHNGSWP.pdf>
- [19] Delicato F.C., Pires P.F., Batista T. *Middleware Solutions for the Internet of Things*, Springer 2013
- [20] Chabanne H., Urien P., Susini J.-F. (eds) *RFID and the Internet of Things*. ISTE LTD and John Wiley & Sons, London 2011
- [21] Kagermann H., Lukas W.-D., Wahlster W. *Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution* <http://www.vdi-nachrichten.com/Technik-Gesellschaft/Industrie-40-Mit-Internet-Dinge-Weg-4-industriellen-Revolution>
- [22] Brettel M., Friederichsen N., Keler M., Rosenberg M. *How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective*. “International Journal of Information and Communication Engineering” 2014, 8, 1:37-44
- [23] Lasi H., Fettke P., Kemper H.-G., Feld T., Hoffman M. *Industry 4.0*. “Business & Information Systems Engineering” 2014, 6, 4:239-242
- [24] Atzori L., Iera A., Morabito G. *The Internet of Things: A survey*, *Computer Networks*. 2010, 54:2787-2805
- [25] Wortmann F., Flucher K. *Internet of Things: A technology added*. “Business & Information Systems Engineering” 2015, 57, 3:221-224
- [26] Smejda P. *Internet rzeczy (IoT) we współczesnej gospodarce. Rola, zadania i bariery rozwoju*. „Zeszyty Naukowe. Organizacja i Zarządzanie”, Politechnika Łódzka 2016, 64:43-55
- [27] Kobylński A. *Internet przedmiotów: szanse i zagrożenia*. „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług”. 2014, 12, 1:101-109
- [28] Rykowski J., Nomańczuk M. *Boje lokalizacyjne – nowy sposób określania położenia wewnątrz budynków*. „Napędy i Sterowanie” 2015, 12:93-100
- [29] Morzyński L., Szczepański G. *Model systemu zdalnego monitoringu parametrów wibroakustycznych środowiska pracy*. „Bezpieczeństwo Pracy. Nauka i Praktyka” 2017, 54, 4:16-20 DOI: 10.5604/01.3001.0009.8780

Publikacja opracowana na podstawie wyników IV etapu programu wieloletniego pn. „Poprawa bezpieczeństwa i warunków pracy”, finansowanego w latach 2017-2019 w zakresie zadań służb państwowych przez Ministerstwo Rodziny, Pracy i Polityki Społecznej. Koordynator programu: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.