IoT W POLSKIEJ GOSPODARCE

RAPORT GRUPY ROBOCZEJ DO SPRAW INTERNETU RZECZY
PRZY MINISTERSTWIE CYFRYZACJI

Ministerstwo
Cyfryzacji

Spis treści

Wydanie 1
Oddano do druku: kwiecień 2019 r.
Wydrukowano w nakładzie 200 egzemplarzy.
Wersja elektroniczna dostępna na www.gov.pl/cyfryzacja

Raport powstał dzięki pracy członków Grupy Roboczej ds. Internetu Rzeczy składającej się z ekspertów działających *pro publico bono* na zaproszenie Ministra Cyfryzacji od 24 sierpnia 2018 r.

Pracom grupy przewodniczyli - Leszek Maśniak i dr Maciej Kawecki – Ministerstwo Cyfryzacji.

Zespół redakcyjny
Ministerstwo Cyfryzacji:
Leszek Maśniak
Katarzyna Marcisz
Jakub Płodzich
Ewa Świętochowska
Anna Tomala
Jan Zaboklicki

Polska Izba Informatyki i Telekomunikacji (PIIT):
Borys Stokalski, lider strumienia IoT w Zespole zadaniowym KRMC „Od papierowej do cyfrowej Polski”
Michał Gałagus

Liderzy podgrup branżowych:
Krystian Bień, Polpharma sp. z o.o.
Aleksander P. Czarnowski, AVET Information and Network Security Sp. z o.o.
Tomasz Dylik, Exatel
Paweł Gora, Uniwersytet Warszawski, Wydział Matematyki, Informatyki i Mechaniki
Damian Hajduk, doradztwo strategiczne i zarządzanie w transporcie i logistyce
Michalski Mateusz, mTechnology /Stowarzyszenie Hackerspace Wrocław
Piotr Mieczkowski, Fundacja Digital Poland
Kamil Nawrocki, BConnect
Marcin Płóciennik, Poznańskie Centrum Superkomputerowo Sieciowe (PCSS IChB PAN)
Jaroslaw Smulski, IDC Poland & Baltic States
Krzysztof Wadas, Grupa Cyfrowy Polsat
Remigiusz Wiśniewski, Detecon International
Marcin Wolski, startup Billon Group ltd.
Marek Zamłyński (do 2018 r.)

Instytucja koordynująca
Ministerstwo Cyfryzacji

Instytucje publiczne wspierające działania Grupy:
Ministerstwo Infrastruktury
Ministerstwo Inwestycji i Rozwoju
Ministerstwo Przedsiębiorczości i Technologii
Główny Urząd Geodezji i Kartografii
Instytut Łączności - Państwowy Instytut Badawczy
Instytut Technik Innowacyjnych ITI EMAG
Urząd Lotnictwa Cywilnego

Główny Partner Biznesowy:
PIIT
Polska Izba Informatyki i Telekomunikacji

Partner Merytoryczny:
digitalpoland
Fundacja Digital Poland

Skład i projekt graficzny: NAŁ Albert Łukasiak
Druk: Drukarnia Offsetowa Express Druk
Sfinansowano ze środków budżetowych Ministerstwa Cyfryzacji

Szanowni Państwo,

tych kilku słów wprowadzenia nie sposób zacząć inaczej niż od podziękowań. Prezentowany raport to efekt dobrej współpracy ponad setki przedstawicieli biznesu i nauki z administracją publiczną. Nie tylko jako szef instytucji, która miała zaszczyt i przyjemność być gospodarzem działań grupy, ale również jako przedstawiciel rządu, do którego jest adresowany ten głos, bardzo serdecznie wszystkim Państwu dziękuję.

Technologie teleinformatyczne to najbardziej obiecujący kierunek rozwoju kraju, w tym – administracji publicznej. To dyscyplina niezwykle dynamiczna, wciąż zaskakująca zasięgiem swojego wpływu na życie społeczne i gospodarcze. Najtęższe głowy nie zdołały trafnie przewidzieć świata, jaki dziś nas otacza i musimy sobie otwarcie powiedzieć, że nie umiemy precyzyjnie określić, co jeszcze technologia nam przyniesie. W działaniach rządu dotyczących nowych technologii konieczne jest zatem przyjęcie bardziej zwinnego podejścia niż dla innych, wolniej zmiennych obszarów. Oznacza to między innymi szersze stosowanie tzw. inteligentnego prawa, czyli takiego, które zamiast arbitralnego wskazywania konkretnych technik czy działań, określa raczej cele i zasady postępowania, które mogą być stosowane mimo postępujących zmian otoczenia. Taka jest konstrukcja zarówno prawa ochrony danych osobowych, jak i konstytucji dla biznesu, czy krajowego systemu cyberbezpieczeństwa.

Drugim warunkiem zwinności, który jako Minister Cyfryzacji uważam za element konieczny, jest stała aktywna współpraca ze środowiskami biznesowymi i naukowymi, bo to one widzą na bieżąco zarówno nowe możliwości, jak i nowe zagrożenia związane z teleinformatyką. Jako rząd mamy wiele budujących przykładów, jak skuteczna jest taka współpraca i jak ważny jest głos społeczeństwa w kształtowaniu prawa i działaniach instytucji rządowych. W ramach Ministerstwa Cyfryzacji działa aktywnie, na różnych poziomach zaawansowania, kilka grup roboczych z dominującym udziałem środowisk biznesowych, prawniczych i naukowych. Są to m.in. grupa ds. sztucznej inteligencji, ochrony danych osobowych, technologii blockchain.

Powołana w sierpniu 2018 r. grupa ds. Internetu Rzeczy, w ciągu 6 miesięcy – mimo ogromnej różnorodności firm i instytucji uczestniczących – opracowała wspólne stanowisko, które z przyjemnością publikujemy na kolejnych stronach raportu. Po raz kolejny udowodnili Państwo, że w dziedzinie rozwoju kraju i stymulowania innowacyjności gospodarki nawet bezpośredni konkurenci mają wspólny interes, a co najważniejsze – że priorytety działania rządu mogą pozostawać w harmonii z oczekiwaniami obywateli i przedsiębiorców.

Państwa głos jest cenny. Docenia i dostrzega go nie tylko Ministerstwo Cyfryzacji. Także inne ministerstwa zadeklarowały gotowość do ścisłej współpracy, by jak najlepiej wykorzystać płynące od Państwa sugestie.

Na koniec… prosimy o więcej. Niezmiennie zachęcamy do aktywnego udziału w obecnych i nowych inicjatywach rządowych i samorządowych, grupach roboczych, konsultacjach i partnerstwach oraz do korzystania z programów wsparcia. Polska nie tylko może być, ale realnie jest ważnym centrum kompetencji teleinformatycznych i warto to wykorzystać.

Marek Zagórski
Minister Cyfryzacji

WARSZAWA, 23 KWIETNIA 2019 R.

01

O RAPORCIE

Grupa robocza ds. Internetu Rzeczy (ang. *Internet of Things – IoT*) została powołana w odpowiedzi na zmieniające się otoczenie technologiczne i rosnącą rolę nowych technologii w pobudzaniu wzrostu gospodarczego. Głównym celem Grupy jest wypracowanie rekomendacji działań, jakie rząd RP powinien podjąć dla zapewnienia warunków rozwoju i upowszechnienia wykorzystania technologii IoT, bazujących na polskiej myśli technicznej, służących poprawie jakości życia w Polsce oraz zagwarantowaniu przewagi konkurencyjnej polskiej gospodarki na rynkach międzynarodowych, ze szczególnym uwzględnieniem wsparcia promocji polskich innowacyjnych firm na świecie. Prace Grupy koncentrują się na następujących obszarach:

- analiza potrzeb polskiej gospodarki związanych z zastosowaniem IoT i wskazanie konkretnych rozwiązań, które powinny być wdrożone na szczeblu ministerstwa i rządu,
- wsparcie w wypracowaniu przez ministerstwo rozwiązań, mających stymulować rozwój firm, produktów i usług związanych z IoT,
- wskazanie barier prawnych, ograniczających rozwój IoT,
- zdefiniowanie obszarów wymagających wprowadzenia standardów i regulacji dla harmonizacji tej części rynku.

W pracach Grupy uczestniczyli eksperci reprezentujący firmy inwestujące w produkty i usługi związane z IoT w Polsce oraz sektory gospodarki, których rozwój jest uzależniony od tych rozwiązań. W stale uzupełniany skład Grupy weszli też przedstawiciele branżowych izb gospodarczych, środowisk naukowych, związków i zrzeszeń pracodawców oraz organizacji społecznych.

Grupa Robocza ds. IoT, przygotowując niniejszy raport, postawiła sobie za cel opisanie aktualnego stanu instytucjonalno-prawnego oraz otoczenia biznesowego branży IoT, wraz z rekomendacjami, których wypełnienie przyczyni się do istotnych korzyści dla polskiej gospodarki, wynikających z implementacji technologii Internetu Rzeczy. Raport identyfikuje również sektory, w których stosowanie technologii IoT może przynieść wymierne korzyści dla obywateli, przedsiębiorstw, samorządów i państwa, w znaczący sposób przyczyniając się do poprawy jakości życia w Polsce.

Prace toczyły się w 10 podgrupach:

Ogólna
Liderzy: Marek Zamłyński (do grudnia 2018 r.), Piotr Mieczkowski, Fundacja Digital Poland i Jaroslaw Smulski, IDC Poland & Baltic States

Bezpieczeństwo i Certyfikacja
Lider: Aleksander P. Czarnowski, AVET Information and Network Security Sp. z o.o.

Finansów i Ubezpieczeń
Lider: Marcin Wolski, startup Billon Group ltd.

Inteligentne Miasta i Budynki
Lider: Remigiusz Wiśniewski, Country Manager, Detecon International GmbH

Ochrona Zdrowia
Lider: Krystian Bień, Polpharma sp. z o.o.

Inteligentne Opomiarowanie
Lider: Krzysztof Wadas, Grupa Cyfrowy Polsat

Przemysł
Lider: Kamil Nawrocki, BConnect

Rolnictwo i Ochrona Środowiska
Lider: Marcin Płóciennik, Poznańskie Centrum Superkomputerowo Sieciowe (PCSS IChB PAN)

Telekomunikacja
Liderzy: Tomasz Dylik, Exatel i Michalski Mateusz, mTechnology i Stowarzyszenie Hackerspace Wrocław

Transport, Logistyka i Pojazdy Autonomiczne
Liderzy: Paweł Gora, Uniwersytet Warszawski, Wydział Matematyki, Informatyki i Mechaniki i Damian Hajduk, doradztwo i zarządzanie w transporcie i logistyce

02
STRESZCZENIE

Internet Rzeczy w kontekście narodowych strategii technologicznych

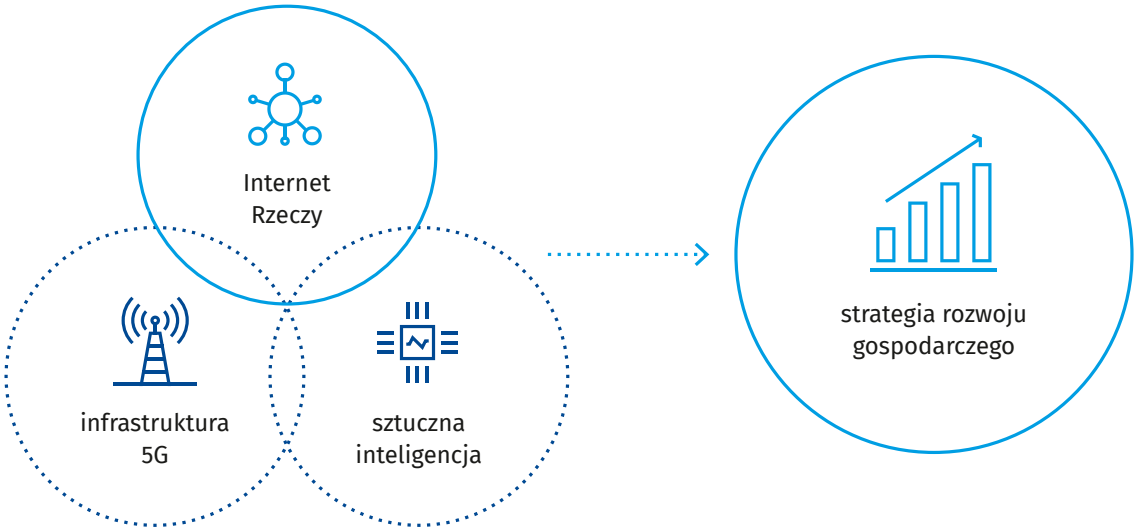
Raport zawiera opis potencjału, jaki drzemie w technologii IoT z punktu widzenia priorytetów rozwojowych polskiej gospodarki. Prezentuje zidentyfikowane bariery i propozycje ich usunięcia, dzięki czemu potencjał ten może zostać uwolniony. Opracowanie zawiera przegląd globalnych trendów, koncentrując się na wyciągnięciu wniosków z obserwowanych zjawisk oraz rekomendacji dla Polski w najważniejszych aspektach związanych z rozwojem systemów IoT: regulacji prawnych, edukacji oraz etyki.

Należy podkreślić, że mówiąc o rozwoju Internetu Rzeczy, mówimy o fali innowacji wykorzystujących sieć inteligentnych przedmiotów, (obiektów wyposażonych w zdolność do przetwarzania danych i kooperacji) której istotą jest nie tylko zaspokajanie znanych dzisiaj potrzeb. Podobnie jak miało to miejsce w przypadku pierwszej „rewolucji internetowej" mamy również do czynienia z kreowaniem nowych obszarów zastosowań, nieoczekiwanych zachowań konsumenckich i nowych modeli biznesowych. Jest to z pewnością obszar ogromnych szans, choć również wielkiego ryzyka charakterystycznego dla masowych fal innowacji. Próbując pokazać kierunki, jakie dziś wydają się najbardziej obiecujące, skazani jesteśmy na ekstrapolację tego, co znamy i spekulowanie na temat tego, co nadejść może.

Dlatego niniejszy raport powinien być regularnie aktualizowany, aby zachować swoją wartość jako przewodnik i materiał wspierający formułowanie strategii technologicznych, które zagospodarują rozwój Internetu Rzeczy. Ten proces aktualizacji powinien być koordynowany z dwoma kierunkami ściśle związanymi z Internetem Rzeczy – narodowymi planami dotyczącymi rozwoju sztucznej inteligencji oraz programem budowy sieci 5G. Są to obszary ściśle ze sobą powiązane i wymagające harmonizacji również w kontekście planów rozwoju gospodarczego, dla których stanowią kluczowy czynnik wspierający.

Przyglądając się inicjatywom powstającym w Polsce i na świecie, powtarzamy za Wiliamem Gibsonem – przyszłość już nadeszła, jest tylko nierównomiernie rozłożona.

Kontekst koncepcji rozwoju Internetu Rzeczy



Potencjał przemysłu teleinformatycznego i elektronicznego

Rozwój produktów i usług IoT wymaga w pierwszej kolejności innowacyjnych koncepcji modeli wartości i modeli biznesowych. Temu zagadnieniu poświęcona jest perspektywa branżowa niniejszego raportu. Ich wytworzenie oraz wdrażanie to z kolei kwestia odpowiedniego potencjału przemysłów teleinformatycznego i elektronicznego. Dlatego istotną częścią opracowania jest diagnoza potencjału polskich firm tworzących szeroko rozumiany sektor „produktów i usług cyfrowych". Dostępne dane i doświadczenie ekspertów branżowych wskazują, że mamy w tym aspekcie dobrą pozycję wyjściową zarówno z punktu widzenia kompetencji technologicznych, jak i z punktu widzenia liczby i dynamiki firm zdolnych do tworzenia rozwiązań IoT. O tym, czy uda się ten potencjał skutecznie i efektywnie zagospodarować, przesądzi tempo transformacji przemysłu teleinformatycznego i elektronicznego z modelu usług integracyjnych i podwykonawstwa komponentów w stronę firm produktowych, kierujących ofertę do końcowych klientów na globalnym rynku. Wsparcie tej transformacji poprzez dyplomację technologiczną oraz programy finansowania wdrożeń innowacyjnych rozwiązań u klientów końcowych wydają się dziś najważniejszymi działaniami, które państwo może podjąć dla wsparcia rozwoju rynku IoT.

Perspektywa branżowa i wspólne wnioski

Istotną częścią opracowania jest szczegółowa charakterystyka branż, które uznano za szczególnie obiecujące w kontekście rozwoju IoT w Polsce. Należy podkreślić, że w większości z nich polscy przedsiębiorcy i inżynierowie tworzą dzisiaj konkretne rozwiązania i produkty wpisujące się w globalne trendy IoT.

W ramach każdej z nich zidentyfikowano konkretne prawno-instytucjonalne przeszkody stojące na drodze upowszechnienia stosowania rozwiązań IoT. Autorzy przedstawiają też propozycje rozwiązań, które będą pomocne w usunięciu tych barier. Wnioski końcowe to ogólne rekomendacje horyzontalne, których zastosowanie pozwoli uwolnić pełny potencjał gospodarki opartej na Internecie Rzeczy.

W toku prac Grupy zidentyfikowano szereg problemów wspólnych dla wszystkich branż:

- Brak edukacji kierunkowej i specjalistycznej – obecnie tylko pojedyncze uczelnie oferują specjalizacje związane z IoT, co może przełożyć się na brak możliwości sprostania rosnącemu zapotrzebowaniu na wykwalifikowane kadry w tej dziedzinie.

- Brak zamówień na rozwiązania IoT ze strony dużych spółek Skarbu Państwa – problem ze skalowaniem rozwiązań na rodzimym rynku przez polskich producentów systemów IoT.

- Brak ewidencji nowatorskich i wdrożonych prototypowych rozwiązań – asymetria informacji, ograniczająca wymianę wiedzy pomiędzy uczestnikami rynku.

- Nieprecyzyjne ramy prawne dotyczące IoT - zagadnienia IoT rozproszone pomiędzy wieloma aktami prawnymi bez zachowania spójności.

- Obecne zastosowania (głównie w sektorze logistyki i ochrony mienia) ograniczające się do rozwiązań M2M (z ang. *Machine to Machine*) – może to utrudnić rozwój polskich rozwiązań IoT dla rynku konsumenckiego.

- Obowiązujące przepisy dotyczące gromadzenia, przechowywania, wykorzystywania danych oraz dzielenia się nimi[1] ograniczającą rozwój IoT w Polsce. Jednym z ważniejszych wyzwań natury prawnej powiązanych z danymi są zagadnienia związane z własnością intelektualną. Jako że infrastruktura IoT bazuje na modelu chmurowym (*cloud computing*) oraz koncepcji Big Data, podobnych wyzwań będzie przybywać lawinowo[2].

W uzupełnieniu do rekomendacji branżowych, Grupa ds. IoT proponuje następujące działania, których podjęcie przyniesie dynamiczny rozwój IoT w Polsce:

- Poprawa koordynacji działań agencji rządowych w kontekście IoT i innych nowoczesnych technologii.

- Stworzenie i uruchomienie programu finansowania wdrożeń pilotażowych i referencyjnych dla innowacyjnych rozwiązań IoT o dużym potencjale umiędzynarodowienia (tworzonych zarówno przez startupy IoT, jak i firmy dojrzałe) pozwalające na obniżenie ryzyka innowacji.

- Uregulowanie możliwości wymiany lub komercjalizacji informacji uzyskanych na bazie IoT, w zakresie, który nie narusza podstawowych zasad ochrony danych osobowych, tajemnic sektorowych lub zawodowych.

- Promocja dobrych praktyk i prekursorskich rozwiązań, np. w formie organizowanych przez rząd konkursów wyróżniających wzorcowe firmy IoT.

- Stworzenie programów wspierających jednostki publiczne na poziomie centralnym (finansowanie, wsparcie przy wyborze technologii i wdrażaniu).

- Zwiększenie transparentności działań organów nadzorczych, w tym – w przypadkach, gdy dana kwestia leży w zakresie właściwości kilku z nich – wydawanie wspólnych jednoznacznych objaśnień, będących efektem konsultacji społecznych i uzgodnień między organami.

- Wprowadzenie ulg podatkowych za stosowanie rozwiązań IoT.

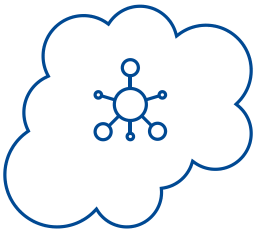
1 McKinsey Global Institute, The Internet of Things: Mapping the value beyond the hype, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

2 Kerr, 2014

03

DEFINICJA INTERNETU RZECZY (IoT)

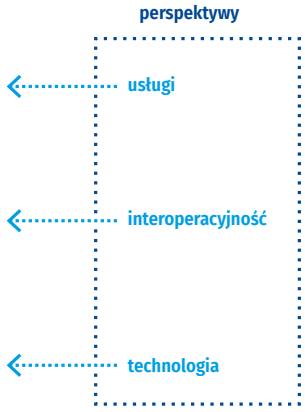
Definicje IoT z różnych perspektyw



Internet Rzeczy jako ekosystem biznesowy
zbiór usług wykorzystujących przedmioty zdolne do zbierania i przetwarzania informacji (interakcji), połączone w sieć, zapewniające interoperacyjność i synergię zastosowań.

Internet of Everything – (Internet wszystkiego – TM Forum)
Urządzenia i produkty konsumenckie podłączone do internetu i wyposażone w rozbudowane funkcjonalności cyfrowe. Koncepcja zakładająca, że przyszłością technologii jest kooperacja urządzeń, przedmiotów i aplikacji włączonych do globalnej sieci.

IoT (Gartner)
Sieć fizycznych obiektów zawierających wbudowaną technologię pozwalającą na komunikację, obserwację zjawisk, manipulację stanem wewnętrznym obiektów oraz wpływanie na ich otoczenie.



Definicja technologiczna

IoT to sieć łącząca przewodowo lub bezprzewodowo urządzenia charakteryzujące się autonomicznym (niewymagającym zaangażowania człowieka) działaniem w zakresie pozyskiwania, udostępniania, przetwarzania danych lub wchodzenia w interakcje z otoczeniem pod wpływem tych danych. Jest to koncepcja budowy sieci telekomunikacyjnych i systemów informatycznych o wysokim stopniu rozproszenia, które służyć mogą między innymi tworzeniu inteligentnych systemów kontrolno-pomiarowych, analitycznych, czy układów sterowania, praktycznie w każdej dziedzinie życia, gospodarki czy nauki.

Definicja architektoniczna

IoT to koncepcja architektury informatycznej, która umożliwia współpracę (interoperacyjność) różnorodnych systemów teleinformatycznych wspierających rozmaite zastosowania dziedzinowe i jest oparta na następujących warstwach:

- Sprzęt – urządzenia (lub przedmioty w nie wyposażone), w szczególności sensory, elementy wykonawcze, ale także sterowniki, smartfony, tablety, laptopy czy komputery, które zdolne są do komunikacji i przetwarzania danych bez zaangażowania człowieka lub w ograniczonej z nim interakcji.
- Komunikacja – infrastruktura telekomunikacyjna oraz sieć telekomunikacyjna (przewodowa lub bezprzewodowa), pracująca w oparciu o dowolne standardy transmisji danych o dowolnym zasięgu (tu Internet).
- Oprogramowanie – systemy informatyczne urządzeń IoT oraz oprogramowanie służące do wymiany danych, ich przetwarzania, zarządzania systemem i jego zabezpieczenia.
- Integracja – zbiory zdefiniowanych usług informatycznych zapewniających interoperacyjność oprogramowania na wszystkich poziomach architektury.

Definicja biznesowa

IoT to ekosystem usług biznesowych, wykorzystujących przedmioty zdolne do zbierania i przetwarzania informacji (interakcji), połączone w sieć, zapewniające interoperacyjność i synergię zastosowań. Łączenie produktów/usług Internetu Rzeczy pozwala na lepsze zrozumienie konsumenta, środowiska, produktów oraz procesów, identyfikację istotnych zdarzeń i reagowanie celem natychmiastowego optymalizowania czy precyzyjniejszej personalizacji.

04

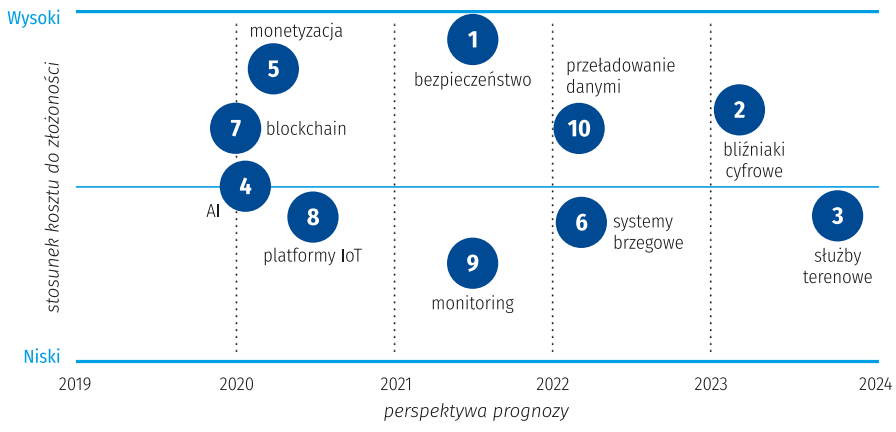
PERSPEKTYWY ROZWOJU BRANŻY IoT NA ŚWIECIE

Najbliższe dwa lata są kluczowe z punktu widzenia przygotowań do zmian, jakie niesie upowszechnienie IoT. IoT wprowadzi istotne zmiany na poziomie większości organizacji, wywołując wzrost popytu na nowe, deficytowe kompetencje (m.in. osób zajmujących się analizą dużych zbiorów danych – **Data Scientist**) oraz tworząc nowe źródła popytu na produkty i usługi przemysłu elektronicznego czy rozwiązania automatyki przemysłowej. Jest to także ostatni moment na wzmocnienie edukacji w tym zakresie, aby lepiej przygotować kadry do zbliżających się wyzwań.

Jak wskazują dane, kulminacyjny punkt adopcji IoT na świecie to 2020 rok. Oznacza to, że Polska i krajowi przedsiębiorcy stoją przed ostatnią szansą dołączenia do wyścigu o najwyższą stawkę. Warto przyjrzeć się następującym zjawiskom IoT, które będą zaprzątać uwagę globalnych graczy rynku IoT w najbliższych miesiącach:

- skupienie się na efektywnych z punktu widzenia zwrotu z inwestycji scenariuszach adopcji IoT oraz dynamiczny wzrost liczby takich scenariuszy,
- ponad 90% wdrożeń IoT będzie opartych o mechanizmy sztucznej inteligencji (ang. *AI – Artificial Intelligence*) i wzrośnie znacząco rola współpracy pomiędzy inżynierami wdrażającymi te rozwiązania, a analitykami danych (*Data Scientists*),
- rynek odczuje istotny deficyt pracowników posiadających potrzebne w omawianych dziedzinach kwalifikacje,
- przewiduje się, że do 2020 roku ponad 70% przedsiębiorstw zainwestuje w infrastrukturę techniczną i zbuduje dla swoich organizacji platformę IoT, czyli stworzy oprogramowanie, którego zadaniem będzie połączenie poszczególnych elementów wchodzących w skład systemu Internetu Rzeczy,
- wzrost zainteresowania możliwościami zastosowania IoT wygeneruje popyt na usługi projektowania i wytwarzania dedykowanych komponentów elektronicznych i elektromechanicznych (czujniki, aktywatory, konsole, autonomiczne urządzenia mobilne i stacjonarne itp.), a liczba takich urządzeń wielokrotnie przekroczy liczbę wykorzystywanych obecnie komputerów stacjonarnych i przenośnych.

Światowe prognozy dla rynku Internetu Rzeczy



Źródło: IDC FutureScape: (Internet of Things, IoT), 2019

Prognoza 1: Ponad 50% firm z krajów G20 do 2021 r. zmodernizuje i otworzy na IoT swoje przemysłowe systemy kontroli produkcji, bez uwzględnienia obaw związanych z bezpieczeństwem IT lub bezpieczeństwem publicznym, co skłoni organy regulacyjne do stanowienia odpowiednich przepisów prawa.

Prognoza 2: Do 2024 r., 50% firm produkcyjnych będzie łączyć odpowiednie bliźniaki cyfrowe (*digital twins*) posiadanych produktów i aktywów, w całościowy ekosystem cyfrowy, aby uzyskać pełen wgląd w biznes na poziomie systemów oraz obniżyć o 5% koszt utrzymania jakości.

Prognoza 3: Pomimo złożoności łańcucha dostaw, utrudniającej innowacje, do 2024 r. 50% producentów wdroży predykcyjne usługi służb terenowych wykorzystujące połączone urządzenia, co przyspieszy realizację usług i zwiększy satysfakcję klienta.

Prognoza 4: Do 2020 r., wskaźnik wdrożonych z sukcesem projektów AI dla rozwiązań IoT osiągnie 90%, przy czym głównym czynnikiem tego sukcesu będzie współpraca między osobami zajmującymi się danymi, a zespołami inżynierskimi.

Prognoza 5: Do 2020 r., ponad 30% inicjatyw IoT na całym świecie nie będzie potrafiła wykazać wyraźnego zwrotu z inwestycji, a organizacje nie będą posiadać niezbędnych wskaźników KPI do monitorowania postępów od wczesnych etapów takich projektów.

Prognoza 6: Ponieważ szacuje się że do 2022 r. 40% wstępnej analizy danych IoT będzie odbywać się w systemach brzegowych (*edge*), organizacje będą więcej inwestować w bramy sieciowe, aby agregować i analizować dane brzegowe, w szczególności w kontekście systemów IT, OT (automatyki przemysłowej) czy CT.

Prognoza 7: W 2019 r. ograniczenia blockchain w przetwarzaniu ogromnej liczby transakcji IoT w czasie rzeczywistym, będą ograniczać integrację IoT z blockchain i związane z IoT wydatki na blockchain do poziomu 5% wszystkich wydatków na tę technologię.

Prognoza 8: Do 2020 r., 70% organizacji będzie wykorzystywać komercyjne platformy IoT do rozwoju i wdrażania aplikacji IoT, a ponad 50% będzie miało środowiska zbudowane z platform IoT pochodzących od wielu dostawców.

Prognoza 9: Do 2021 r., 45% treści pochodzących z monitoringu wideo będzie wykorzystywana do dostarczania danych kontekstowych do danych pochodzących z punktów końcowych IoT w rożnych scenariuszach zapewniania bezpieczeństwa publicznego w takich miejscach jak huby transportowe czy w monitoringu środowisk kampusowych.

Prognoza 10: Do 2022 r., problemy związane z agregacją i racjonalizacją danych pochodzących z sensorów w celu uzyskania sensownych informacji, będzie zmuszać 20% dużych producentów do uzgadniania danych OEM na platformach wymiany danych IoT.

Poziom adopcji Cyfrowej Transformacji w Polsce

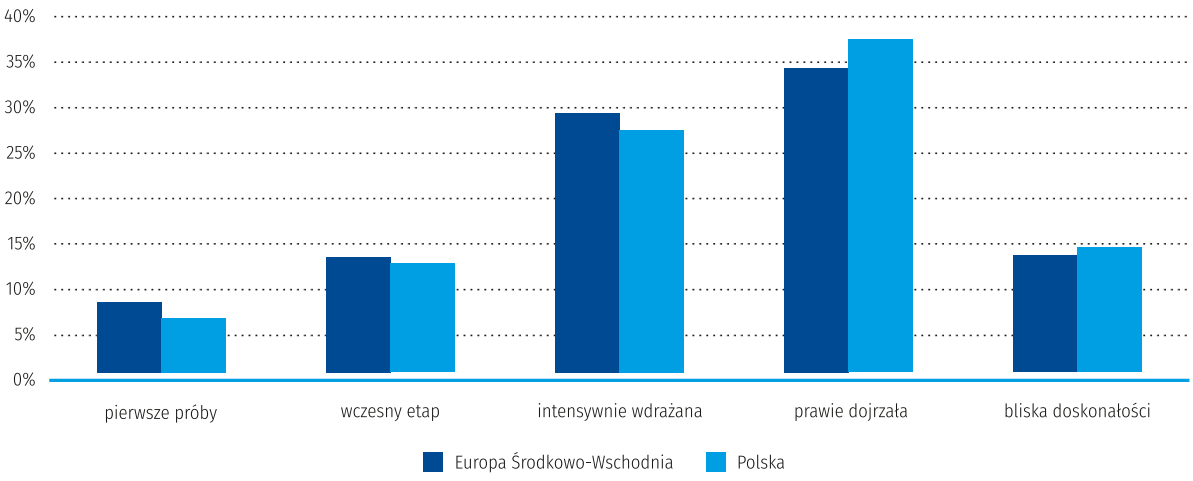
Otwartość polskich organizacji na procesy cyfrowej transformacji wpływa korzystnie na oczekiwany wysoki poziom adopcji IoT na naszym rynku.

Badanie poziomu adopcji cyfrowej transformacji w Polsce wskazuje na zaufanie rodzimych organizacji do tych zjawisk. Choć zaskakująco wysoki poziom ich adopcji w fazie zaawansowanej (*rather developed*), może wynikać z chęci respondentów do zaliczenia siebie do zaawansowanej technologicznie grupy, wynik można potraktować jako przejaw aspiracji naszych firm i dużego zainteresowania polskiego biznesu nowoczesnymi rozwiązaniami cyfrowymi.

IoT jest jednym z elementów cyfrowej transformacji, co więcej – jest podstawą dla technologii przetwarzania danych i ich monetyzacji, technologii predykcyjnych (*ang. Machine Learning, Deep Learning*), czy w końcu AI. Można zatem przyjąć wysoką zależność pomiędzy chęcią adopcji procesów cyfrowej transformacji, a chęcią i otwartością na adopcję IoT.

W najbliższych latach oczekiwane jest wysokie tempo wzrostu rynku technologii i rozwiązań IoT (ok. 13% rok do roku). Oznacza to, że polska gospodarka ma ogromne szanse na absorpcję tej technologii, a jeśli usunąć istniejące ograniczenia, potencjał ten może jeszcze wzrosnąć. Likwidacja barier, m.in. w zakresie regulacji, czy rozwoju nowych technologii komunikacyjnych (w tym **5G**), przyniesie dynamiczny rozwój IoT w Polsce.

Deklarowany poziom adopcji rozwiązań Cyfrowej Transformacji w Polsce na tle Europy Środkowo-Wschodniej



Źródło: IDC CEE Digital Transformation Survey, 2017; N=311

05

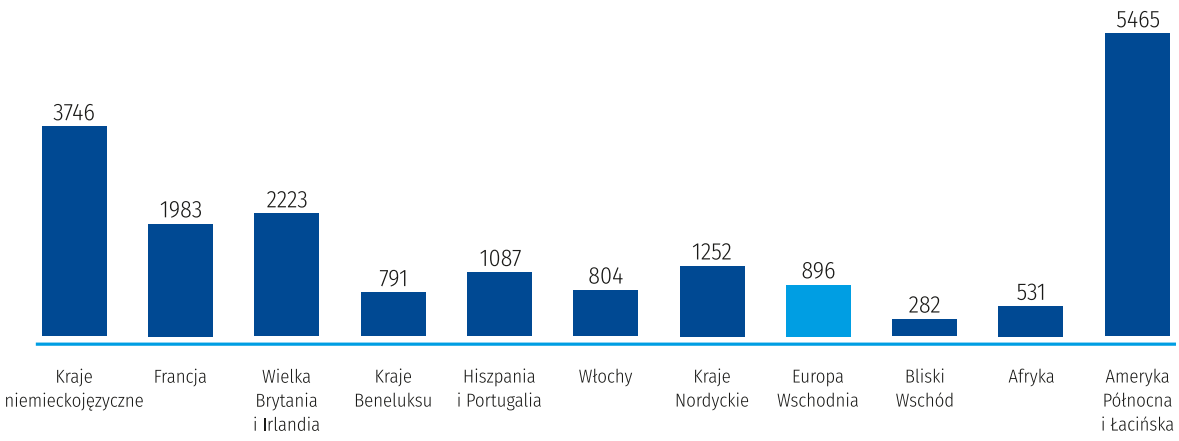
WARUNKI ROZWOJU IoT W POLSCE – DIAGNOZA SYTUACJI

Rynek firm oferujących rozwiązania IoT na podstawie dostępnych statystyk

W Polsce działa wiele firm, oferujących zróżnicowane rozwiązania IoT, dostosowane do potrzeb różnych sektorów gospodarki. Jednak nadal jest ich zbyt mało, podaż jest niewspółmierna do popytu na rozwiązania Internetu Rzeczy. Stworzenie warunków dla dalszego rozwoju firm wychodzących naprzeciw potrzebom jest kluczowe dla rozwoju IoT i w efekcie polskiej gospodarki. Zgodnie z danymi CompuBase[1], pod względem liczby firm oferujących rozwiązania IoT, nasz region plasuje się poniżej poziomu krajów Europy Zachodniej i Ameryki Północnej, ale blisko regionów o podobnym poziomie rozwoju. Co istotne, firm oferujących rozwiązania IoT w Europie Wschodniej jest blisko 900, z czego większość to firmy działające w naszym kraju. Jest ich wystarczająco dużo, aby zaspokoić rosnące potrzeby związane z rozwiązaniami IoT.

Pod względem segmentu, w jakim funkcjonują firmy oferujące rozwiązania IoT, dominujące znaczenie mają przedsiębiorstwa działające w modelu **B2B**, czyli sprzedające oprogramowanie innym przedsiębiorstwom. Stanowią one aż 26% wszystkich podmiotów oferujących rozwiązania IoT. Drugie miejsce zajmują dostawcy usług programistycznych i rozwoju oprogramowania – stanowią 20% firm działających na tym rynku. Te dwa segmenty są najistotniejsze z punktu widzenia działań związanych z IoT, i dlatego działania rządu powinny skupić się na wspieraniu firm, które tworzą własne rozwiązania lub rozwijają istniejące, co przekłada się na rozwój całego rynku.

Liczba firm oferujących rozwiązania IoT na poszczególnych rynkach



Źródło: CompuBase

1 http://en.compubase.net/Companies-working-with-IoT-related-skill-sets_a315.html

Firmy oferujące rozwiązania IoT w podziale na segmenty (na podstawie danych globalnych)

Rodzaj firmy	Odsetek
Producenci	7%
Wydawcy oprogramowania	4%
Wydawcy oprogramowania wykorzystywanego do konkretnych sektorów lub obszarów działalności firm	3%
Wydawcy oprogramowania wykorzystywanego do konkretnych procesów firmy	7%
Integratorzy rozwiązań lub usług programistycznych (tworzonych przez inny podmiot)	2%
Usługi informatyczne, rozwój oprogramowania	20%
Usługi telekomunikacyjne (np. operatorzy telekomunikacyjni, dostawcy usług internetowych)	5%
Integratorzy infrastruktury sieciowej i telekomunikacyjnej	6%
Integratorzy infrastruktury IT	4%
Doradztwo	1%
Sprzedaż rozwiązań klientom indywidualnym	6%
Sprzedaż rozwiązań klientom biznesowym (sprzęt, oprogramowanie i usługi)	26%
Sprzedaży hurtowa (sprzedaż produktów IT i telekomunikacyjnych sprzedawcom detalicznym lub biznesowym)	6%
Agencje sieciowe	0%
Inne działalności związane z obszarem IT i telekomunikacji	1%

Źródło: CompuBase

Potencjał rynku i główne bariery z perspektywy kategorii rozwiązań IoT (analiza jakościowa)

Dotychczas nie wykształcił się uniwersalny model funkcjonowania przedsiębiorstw oferujących rozwiązania IoT. Wiele firm samodzielnie prowadzi cały proces, od stworzenia produktu poprzez marketing, sprzedaż, wdrożenie, serwis i zarządzanie. Są i takie, które zajmują się tylko tą częścią projektu, w której czują się najbardziej kompetentne, resztę zostawiając np. dystrybutorom. Można przy tym coraz wyraźniej wyodrębnić segmenty rynku, odpowiadające różnym poziomom definicji Internetu Rzeczy:

1. Producenci prostych urządzeń interaktywnych, sterowanych poprzez Internet, dedykowanych do określonej kategorii zastosowań (poziom technologiczny):
   - mikronadajniki (ang. *beacony*),
   - czujniki,
   - kamery internetowe,
   - zdalnie sterowane źródła światła, zamki, itp.

   Przykładowi polscy producenci: AIUT, Estimote, Comarch, Action

2. Producenci skomplikowanych urządzeń realizujących złożone funkcje, generujących dane i/lub sterowanych poprzez internet (poziom technologiczny):
   - autonomiczne urządzenia transportowe,
   - roboty przemysłowe,
   - urządzenia mobilne (smartphone, smartwatch itp.),
   - inteligentne, cyfrowe urządzenia pomiarowe.

   Przykładowi polscy producenci: CEIT/Asseco, AIUT, Atende, VersaBox, Flytronics/WB Electronics

3. Twórcy i operatorzy cyfrowych platform i usług biznesowych wykorzystujących urządzenia z warstwy 1 i 2 (poziom architektoniczny i biznesowy):
   - optymalizacja zużycia energii,
   - inteligentny transport,
   - systemy transportu miejskiego,
   - inteligentne systemy parkingowe,
   - rozwiązania **omnichannel**.

   Przykłady: Virtual Power Plant, VersaBox, NextBike Poland, PROPARK, iTaxi

4. Integratorzy rozwiązań IoT (poziom biznesowy):
   - tradycyjne **firmy integratorskie**,
   - firmy realizujące kompleksowe inwestycje inteligentnych budynków,
   - firmy wdrażające złożone systemy pomiarowe,
   - firmy wdrażające kompleksowe rozwiązania robotyzacji produkcji i logistyki.

   Przykłady: Asseco Data Systems, Atende, AKE Robotics, AIUT

Potencjał rynku IoT z perspektywy technologicznej

Urządzenia elektroniczne (wymienione w pkt. 1 i 2) są bazą każdego wdrożenia – to one bowiem umożliwiają „rzeczom" przetwarzanie i przesyłanie informacji. Tymi urządzeniami mogą być skomplikowane układy, jak również pełnowartościowe komputery, jakie znajdziemy w robotach czy pojazdach. Mogą nimi być również proste, masowo produkowane czujniki. W każdym przypadku trzeba zadbać, by posiadały odpowiednią dla zastosowania moc obliczeniową i interfejsy komunikacyjne, a także możliwość efektywnego zasilania.

Możliwości technologiczne produkcji bazowych komponentów elektronicznych i baterii są skupione w wąskim gronie firm globalnych (np. Intel, Samsung) – poza technologią bardzo istotny jest również dostęp do surowców i ich dystrybucja. Produkcja urządzeń elektronicznych to bowiem zaawansowany proces, który wymaga najnowocześniejszych technologii. Najprostsze komponenty, np. kondensatory, rezystory (elementy pasywne) są stosunkowo tanie i proste w produkcji. Komponenty aktywne, do których zaliczają się układy scalone (w tym procesory) to elementy, do których produkcji wymagane jest stosowanie tzw. nanotechnologii. Pierwsze procesory w skali 800 nm były produkowane w roku 1989, obecnie dąży się do „upakowania" tranzystorów na poziomie 5 nm (przewiduje się to w roku 2020).

Od kilku lat najistotniejszym elementem sprzyjającym rozwojowi IoT jest popularyzacja tzw. SOC (ang. *System on a Chip*), które w jednym układzie scalonym zawierają (w uproszczeniu) procesor, pamięć operacyjną, układy komunikacji radiowej, układy analogowe i pamięć flash. Pozwala to uzyskać praktycznie kompletne urządzenie wykonawcze o zredukowanym rozmiarze i dużej funkcjonalności, kosztem najczęściej jedynie pogorszonych parametrów termicznych.

Istnieje spory potencjał dla producentów urządzeń zbudowanych z wielu powszechnie dostępnych i sprawdzonych elementów. Produkcja urządzeń IoT, specyficznych dla danej aplikacji, jest w pełni możliwa w dowolnym zakładzie posiadającym linie montażu elektroniki. Dotychczas obecna była tendencja stosowania outsourcingu produkcyjnego kierowanego w szczególności do krajów azjatyckich, jednak trend ten się odwraca ze względu na coraz większą świadomość technologiczną przedsiębiorstw i chęć posiadania własnych możliwości produkcyjnych. Stanowi to bardzo pozytywny sygnał dla gospodarek lokalnych.

Rynek produkcji elektroniki w Polsce jest postrzegany jako dojrzały i ma spore możliwości, również w kontekście mocy zakupowej, która przy dużych wolumenach produkcji jest bardzo istotna dla zapewnienia terminowości dostaw.

Proces produkcji jest warunkowany również poprzez możliwość śledzenia pojedynczego urządzenia od momentu wprowadzenia na linię produkcyjną komponentów od konkretnych dostawców, poprzez proces składania, kontroli jakości, pakowania, wysyłki i późniejszej instalacji u klienta (ang. *traceability*).

Jakość urządzeń i ich trwałość jest związana nie tylko z zapewnieniem właściwego użycia komponentów, montażu i testowania, ale również z dbałością o odpowiednie środowisko produkcji (np. ochronę antystatyczną na każdym etapie produkcji, czy ochronę przed zanieczyszczeniami).

Kluczowe dla urządzeń IoT jest:

1. Zastosowanie optymalnych komponentów, z punktów widzenia:
   - energochłonności,
   - rozmiaru,
   - mocy obliczeniowej,
   - niezawodności,
   - długowieczności,
   - odporności na skrajne warunki środowiskowe.

2. Zapewnienie certyfikacji.

3. Przygotowanie odpowiedniego projektu i wykonanie płytki PCB (ang. *Printed Circuit Board*), zwanych inaczej płytkami drukowanymi, przeznaczone do montażu podzespołów elektronicznych.

4. Stworzenie obudowy.

5. Sposób zasilania (długowieczne baterie, energia odnawialna).

Urządzenia IoT muszą charakteryzować się kompromisowym podejściem w łączeniu wysokiej mocy obliczeniowej z niskim zapotrzebowaniem na energię, która w wielu aplikacjach może być pozyskiwana jedynie z baterii. Możliwe jest stosowanie źródeł odnawialnych takich jak ogniwa fotowoltaiczne, jak również konwencjonalnych np. baterii litowych. Bardzo istotna jest żywotność ogniw umożliwiająca ciągłość pracy przez wiele lat, a także możliwość oprogramowania urządzenia tak, by było w stanie poinformować użytkownika o konieczności wymiany baterii.

Rynek urządzeń IoT wymusza na producentach możliwość adaptacji do różnych potrzeb. Istnieje konieczność produkowania wielu wersji urządzeń np. pod kątem zróżnicowanych metod zasilania, czy interfejsów komunikacyjnych, włączając w to różne anteny. Elastyczność producentów powinna przejawiać się możliwością szybkiego prototypowania i krótkiego czasu wdrażania liczonego od przygotowania prototypu do wprowadzenia urządzenia do masowej produkcji. Jest to również związane z możliwością prostej i niezawodnej instalacji oprogramowania oraz certyfikacji. Duże znaczenie ma coraz powszechniejsze stosowanie druku 3D do tworzenia prototypów obudów.

Opaska dla seniorów firmy SiDLY monitorująca aktywność oraz parametry życiowe.

Autonomiczny robot mobilny firmy Versabox stanowiący element platformy automatyzującej procesy logistyki wewnętrznej AUTONOMY@WORK.

Liderami branży są firmy, które potrafią produkować własne urządzenia i oprogramowanie, utrzymując pełną kontrolę nad każdym aspektem operacyjności, zarówno swojego sprzętu, jak i całego systemu.

Z racji na powyższe uwarunkowania, branżę elektroniczną w Polsce cechuje duży udział kapitału zagranicznego, reprezentowanego przez takich potentatów światowych jak np. JabilCircuit, Royal Philips Electronic, LG, Samsung, czy Motorola. Konsekwencją tego stanu rzeczy jest funkcjonowanie licznej grupy polskich przedsiębiorców w roli poddostawców globalnych firm. Paradoksalnie, polskie przedsiębiorstwa są jednocześnie klientami tych firm, jeśli chodzi o podstawowe komponenty. Przekłada się to na spadek rentowności produkcji w polskich zakładach, co potwierdza fakt ujemnego salda wymiany zagranicznej Polski w zakresie wyrobów wysokiej techniki, wynoszące według wyliczeń Eurostatu z 2015 r. 6,8 mld euro, z czego 3,1 mld euro przypadało na wymianę z państwami UE[2].

Wymagania wobec współczesnej elektroniki i elektrotechniki, w zakresie jej zaawansowania technologicznego wciąż rosną. Można to porównać do wyścigu, w którym wszyscy jego uczestnicy wciąż zwiększają tempo biegu, przekraczając kolejne granice i bijąc poprzednie rekordy. Wyraża się to w głównej mierze w miniaturyzacji podzespołów i kompletnych wyrobów, przy jednoczesnej poprawie ich parametrów, a także dodawaniu nowych funkcji. Oznacza to, że nie zawsze producenci sprzętu są w stanie spełnić wyśrubowane wymagania w całym asortymencie produkcji.

Rynek kieruje coraz więcej wymagań wobec producentów, co prowadzi do konieczności poszukiwania nowych metod ich spełnienia. Jednym z tego typu modeli jest wykorzystanie outsourcingu zarówno konkretnych podzespołów, jak i całych urządzeń elektronicznych. Wyspecjalizowane firmy świadczące usługi montażu na zlecenie np. Electronic Manufacturing Services – EMS, są na ogół dobrze wyposażone w sprzęt i technologie w ściśle określonym zakresie, przez co mogą wykorzystać pełnię możliwości specjalizacji i stale dostosowywać się do zmiennych warunków rynkowych. Dzięki temu mogą również realizować złożone technologicznie operacje, np. automatyczną inspekcję optyczną, pozwalającą sprawdzić jakość montażu elementów w obudowach drukowanych po obu stronach płytek PCB.

Poprzez skorzystanie z usług EMS, firmy zajmujące się sprzedażą wyrobów elektronicznych i elektrycznych pod własną marką, mogą skupić się na rozwoju swojej podstawowej działalności. Istotną korzyścią są również niższe nakłady inwestycyjne wymagane do rozpoczęcia produkcji, a także możliwość bardziej elastycznego dostosowania asortymentu do potrzeb rynkowych. Zalety wynikające z korzystania z usług firm zewnętrznych widać szczególnie wyraźnie w przypadku krótkich i średnich serii produkcyjnych.

Według wyników badań zaprezentowanych w Informatorze Rynku Elektroniki 2017, potrzeby przedsiębiorców korzystających z usług outsourcingu znacznie przekraczają jedynie proces montażu. Badane firmy wskazują m.in. na zakup podzespołów, testowanie i uruchamianie gotowych wyrobów, wykonanie płytek

2 A. Ostrowski: Przemysł elektroniczny i elektrotechniczny w Polsce – raport, 17.10.2017, opublikowany na stronie internetowej: www.magazynprzemyslowy.pl/zarzadzanie-i-rynek/Przemysl-elektroniczny-i-elektrotechniczny-w-Polsce-raport,9970,1

drukowanych i szablonów, a także usługi projektowe i wsparcie techniczne[3].

Same firmy EMS muszą antycypować zmiany rynkowe, wprowadzając nowe usługi do swojej oferty. Wymaga to na nich reakcję na niewyartykułowane jeszcze potrzeby nabywców. Związane jest to z koniecznością przewidywania potencjalnych zagrożeń, z którymi wytwórcy urządzeń elektronicznych i elektrycznych mogą się spotkać, w wyniku ograniczeń kosztowych i technologicznych.

Grupa przedsiębiorców zajmujących się w Polsce produkcją elektroniki na zlecenie liczy ponad 100 firm różnej wielkości i o szerokiej skali działania[4]. Wielu producentów elektroniki lub elektrotechniki wciąż wytwarza swoje produkty we własnym zakresie, korzystając z własnych zasobów i linii produkcyjnych. Przywiązują oni większą wagę do kontroli nad całym procesem produkcji, ochronę własności intelektualnej, czy stałego rozwoju potencjału produkcyjnego firmy. Jednak rosnąca presja ze strony rynku oraz znaczący potencjał ekonomiczny wykorzystywania usług EMS będą sprzyjały rozwojowi tego segmentu w przyszłości.

Obecnie polskie firmy EMS skupiają się na świadczeniu usług dla klientów zagranicznych, głównie z Europy Zachodniej i krajów skandynawskich. O ich przewadze świadczą niższe koszty, wykwalifikowana kadra produkcyjna, wysoki poziom zaawansowania technologicznego, czy bliskość geograficzna. Firmy te są jednak pod stałą presją wynikającą z sytuacji na rynku pracy, przez co będą musiały stale podnosić jakość swoich usług.

Internet Rzeczy tworzy szansę dla polskich producentów, otwierając zupełnie nowe klasy zastosowań pozwalające na innowacyjne wykorzystanie bazowych komponentów i przetwarzanie ich w produkty dla końcowych klientów. W szczególności, ze względu na przewidywany duży wolumen dostaw, konieczność długoletniej eksploatacji urządzeń i zapewnienia serwisu z częściami zamiennymi, rynek IoT będzie wyjątkowo atrakcyjny dla producentów sprzętu elektronicznego.

Odpowiedni łańcuch dostaw komponentów do produkcji urządzeń staje się zatem krytyczny. Współcześnie, większość elementów IoT jest produkowana jako osobne, niezależne urządzenia spełniające określoną funkcję, pracujące w pewnych specyficznych warunkach środowiskowych, na które składa się dostępność zasilania i mediów komunikacyjnych, temperatura, czy wilgotność. Przewiduje się, że w najbliższym czasie zacznie następować integracja IoT z innymi urządzeniami powszechnie już stosowanymi – przykładem są lampy zarówno uliczne, jak i domowe, znaki drogowe, samochody, ubrania i szereg innych. Będzie się to wiązało ze stosowaniem nowych materiałów i kooperacją między wytwórcami.

Produkcja elektroniki jest od lat zdominowana przez kraje azjatyckie, głównie Chiny. Wielkie zakłady produkcyjne Azji charakteryzują się niemal nieskończonym poziomem chłonności komponentów elektronicznych. Co przekłada się na zaburzenie światowych rynków. Z punktu widzenia struktury rynku, znaczącym problemem są więc potencjalne trudności w zakupie komponentów potrzebnych do produkcji urządzenia końcowego. Koszt zakupu elementów dostępnych „od ręki" jest zbyt wysoki wobec konieczności zachowania konkurencyjności. Na rynku istnieje tylko kilku brokerów, u których można zamawiać elementy bazowe. Wpływa to również na terminy realizacji zamówień, szczególnie najpopularniejszych podzespołów, takich jak SOC, czy kondensatory.

Produkcja elektroniki będzie związana ze stałym podnoszeniem jakości, coraz krótszymi terminami dostaw nowych urządzeń i konkurencją cenową, która będzie eliminować z rynku niewielkich „graczy". Start-up'y posiadające dobre projekty urządzeń będą zmuszone do kooperacji z większymi podmiotami posiadającymi realne możliwości produkcyjne. Będzie się to wiązało z zabezpieczeniem interesów poprzez odpowiednie postępowania patentowe. Klienci aplikacji, szczególnie tych najpopularniejszych, będą oczekiwali możliwości wzięcia w leasing urządzeń z pełnym zapleczem serwisowym.

W zakresie IoT, kluczowe będzie również wykorzystanie najnowocześniejszych rozwiązań w zakresie sprzętu elektronicznego. Na rynku coraz częściej identyfikuje się potrzebę wykorzystywania tzw. elektroniki high-tech, czyli np. elastycznych płytek PCB (tzw. fleksy), które umożliwią instalowanie sensorów np. w ubraniach, bez ryzyka ich pęknięcia.

Wdrażanie do produkcji nowych urządzeń jest również ściśle związane z dostępnością wydajniejszych technologii zasilania. Trwają prace nad mikro-ogniwami wodorowymi, bateriami grafenowymi, czy perowskitami, stanowiącymi alternatywę dla krzemowych ogniw słonecznych). Ze względu na trudności z zapewnieniem odpowiednich baterii dla rosnącego rynku IoT (i nie tylko), Polska powinna zainwestować w zaplecze surowcowe i postawić na produkcję ogniw. Już obecnie istnieją w Polsce firmy posiadające zdolność zakupu działek wydobywczych na całym świecie.

Oprócz ograniczeń natury rynkowej wspomnianych powyżej, Grupa zidentyfikowała również inne istotne bariery dla rozwoju branży elektronicznej z punktu widzenia rozwiązań IoT:

3 www.elektronikab2b.pl/download/Informator_Rynkowy_Elektroniki_2017.pdf
4 Ibidem

- Brak specyfikacji rozwiązań IoT dla instytucji publicznych, utrudniający realizowanie zamówień przez sektor publiczny. Niemożność stworzenia tzw. SIWZ (Specyfikacja Istotnych Warunków Zamówienia) wynika z braku referencyjnych projektów, stanowiących odpowiedni **benchmark technologiczny**.

- Konieczność zapewnienia w ofercie na zamówienie publiczne restrykcyjnych warunków gwarancji, co sprawia, że na producencie rozwiązania (ewentualnie na dostawcy lub integratorze) spoczywa praktycznie pełna odpowiedzialność za awarie urządzeń. W związku z tym, do przetargów mogą stawać jedynie duże firmy, które są w stanie ponieść wysokie koszty ewentualnych napraw i konserwacji. W przypadku IoT, bardzo dużym problemem mogą stać się również odległości między poszczególnymi urządzeniami tworzącymi system, przekładające się wprost na wysokie koszty transportu.

- Wysokie koszty związane ze stosowaniem nowoczesnych metod tworzenia obudowy urządzeń. Tzw. produktyzacja urządzeń ściśle wiąże się z wytworzeniem obudowy. Na potrzeby przygotowania prototypów odpowiada druk 3D, natomiast myśląc o produkcji seryjnej należy stosować formy wtryskowe, których koszt jest wysoki, przekraczając często możliwości finansowe mniejszych podmiotów.

- Procedury i koszty badań urządzeń pod kątem EMC (ang. *Electromagnetic Compatibility*) oraz ich certyfikacji.

- Rosnąca presja na polskie firmy oferujące rozwiązania IoT, związane ze stałym podnoszeniem jakości, terminowości dostaw oraz zapewnieniem interoperacyjności, tak aby były one konkurencyjne względem rozwiązań dostępnych na rynkach zagranicznych.

Potencjał rynku IoT z perspektywy architektonicznej i biznesowej

Dla firm działających w kategorii 1 i 2 powyższej „mapy rynku", podstawową barierą jest zdolność do tworzenia „ekosystemów zastosowań". Oferowane przez firmy produkty są zaledwie jednym ze składników biznesowych rozwiązań IoT – same w sobie nie oferują zwykle wartości, za którą mógłby zapłacić klient końcowy. Nawet urządzenia konsumenckie – np. tworzące ofertę „**smart home**" – nabierają wartości dopiero wtedy, gdy ktoś zintegruje je w ekosystem, realizujący konkretne potrzeby domowników, bez absorbowania ich koniecznością nieustannej interakcji z technologią. Z drugiej strony dynamika rynków technologicznych sprawia, że inwestorów przyciągają dziś przede wszystkim produkty dające szansę na wdrożenie w skali międzynarodowej. Kompetencje tworzenia złożonych rozwiązań, ekosystemów usług odpowiadających punktom 3 i 4 z powyższej mapy rynku są reprezentowane w największej mierze przez duże firmy informatyczne łączące model produktowy z integratorskim oraz przez operatorów telekomunikacyjnych.

Po kilku dekadach dynamicznego **rozwoju rynku IT** opartego o popyt lokalny, zaspokajany przez integrację rozwiązań światowych firm technologicznych, polski rynek ICT przechodzi intensywną transformację, wdrażając strategie produktowe i orientując się na zagraniczną ekspansję. W tym procesie barierą jest brak naturalnych kanałów rozprzestrzeniania, jakim byłby ekosystem polskich firm o międzynarodowej skali działania, poszukujących okazji do modernizacji oferty i poszerzania rynku w oparciu o innowacje. Popyt wewnętrzny jest niewystarczającą siłą do tego, by transformacja sektora ICT przebiegła w szybkim tempie, zaś doświadczeń w umiędzynarodowieniu polskich produktów i usług cyfrowych brakuje.

Z tego punktu widzenia kluczową kwestią jest wsparcie przez instytucje publiczne istniejącego i rozwijającego się rynku polskich produktów IoT w zakresie ich umiędzynarodowienia, poprzez:

- skuteczną dyplomację technologiczną, realizowaną we współpracy ze środowiskiem biznesowym,

- pomoc w działaniach związanych z certyfikacją produktów IoT na rynkach zagranicznych,

- udział w tworzeniu sieci kooperacji z globalnymi podmiotami inwestującymi w Polsce w ośrodki rozwoju własnych produktów i usług IoT,

- powołanie funduszu, mającego na celu zabezpieczenie płynności finansowej firm produkujących lub wdrażających innowacyjne urządzenia elektroniczne niezbędne w systemach IoT. Fundusz ten stanowiłby wsparcie dla mniejszych firm, podejmujących wysokie ryzyko wdrożeń rozwiazań IoT (np. ponadnormatywne koszty konserwacji i modyfikacji prototypowych urządzeń).

- promowanie współpracy dużych firm ze start-upami, dającej możliwość realizowania większych projektów przez młode, rozwijające się przedsiębiorstwa; Kluczem do rozwoju firm z branży jest tworzenie produktów wieloseryjnych, do czego konieczne jest pozyskiwanie dużych zamówień oraz znaczące inwestycje w potencjał produkcyjny,

- wypracowanie ramowych specyfikacji dla rozwiązań IoT dla potencjalnych wdrożeń systemów IoT dla sektora publicznego, co przyspieszy proces realizacji zamówień na tego typu systemy oraz obniży jego koszty.

Bariery popytowe dla rozwoju firm IoT w Polsce

Jedną z istotnych barier, która powstrzymuje wiele firm przed wdrażaniem rozwiązań biznesowych wykorzystujących IoT, jest obawa przed ryzykiem innowacji. Część uczestników rynku woli obserwować

nowy trend, niż przeobrazić swoje procesy biznesowe pod wykorzystanie IoT.

W kontekście IoT istotna jest wielkość przedsiębiorstwa. Według danych CompuBase, 21% firm z **regionu EMEA** aktywnych na rynku IoT zatrudnia ponad 500 osób. Dodatkowo, im mniejszy podmiot, tym rzadziej działa w tym obszarze[5]. Ważne jest więc wspieranie zarówno dużych firm oferujących tego typu rozwiązania, jak i tych mniejszych przedsiębiorstw, które mają potencjał rozwojowy i mogą stać się w niedalekiej przyszłości ważnymi dostawcami rozwiązań IoT.

Koszty mogą stanowić istotną barierę, która utrudnia mniejszym integratorom oferowanie własnych rozwiązań IoT. W szczególności zakup sprzętu, tworzącego infrastrukturę rozwiązania IoT, może oznaczać spory wydatek zarówno dla integratora, jak i klienta końcowego, zaś usługi udostępniania takiej infrastruktury (np. niskoenergetyczne **sieci mesh** dla inteligentnego rolnictwa) są dziś jeszcze słabo dostępne. Może to być bariera nie do pokonania dla mniejszych firm, które często nie mogą sobie pozwolić na ulokowanie sporej części kapitału w urządzenia potrzebne do produkcji systemów IoT, przez co wstrzymują realizację większych projektów.

Tzw. „produktyzacja" urządzeń ściśle wiąże się z wytworzeniem obudowy. Do prototypowania idealny okazuje się druk 3D, natomiast myśląc o produkcji seryjnej należy stosować formy wtryskowe, których koszt jest wysoki, przekraczając często możliwości mniejszych podmiotów.

Znaczącą barierą jest również brak kompetencji związanych z kwestiami powiązanymi z IoT, takimi jak aspekty prawne (np. ochrona prywatności). Wciąż jest niewielu specjalistów na rynku, mogących świadczyć profesjonalne usługi w tym zakresie. W wielu przypadkach firmy te są zmuszone do działania w warunkach wysokiego ryzyka biznesowego lub powolnego kształcenia kompetencji wewnątrz przedsiębiorstwa. Wiele z nich w związku z tym porzuca projekty innowacyjne, skupiając się na podstawowej działalności.

Z tego punktu widzenia kluczowe jest zbudowanie i upowszechnienie mechanizmu finansowania wdrożeń innowacji, w którym finansowanie innowacji realizowane jest poprzez wsparcie średnich, rozwijających się przedsiębiorstw zainteresowanych pilotażem i w przypadku powodzenia pilotażu, wielkoskalowym wdrożeniem innowacji. Finansowanie to powinno obejmować budowę kompetencji po stronie organizacji wdrażającej innowację jako warunek niezbędny do uzyskania przez nią finansowania.

Również bariery o charakterze behawioralnym mogą odgrywać istotną rolę w kontekście rozwoju systemów opartych na koncepcji Internetu Rzeczy. Wiążą się one z takimi aspektami, jak kwestie postaw konsumentów w kontekście akceptacji bądź jej braku, określone rozwiązania IoT ze względu np. na zaufanie do nich. Warto zwrócić uwagę na jeszcze jeden obszar mogący mieć istotne znaczenie dla rozwoju Internetu Rzeczy – kwestie zmian strukturalnych.

Środowisko regulacyjne

Środowisko regulacyjne w Polsce nie tylko nie sprzyja rozwojowi systemów IoT, ale wręcz stanowi dla niego istotne ograniczenie. W polskim systemie prawnym brak jest odrębnych i szczegółowych regulacji dla technologii IoT. Rozproszone po wielu aktach prawnych (m.in. **RODO**, prawo telekomunikacyjne i tajemnice sektorowe, **NIS**) regulacje dotyczące IoT, często nadają organom administrującym lub nadzorczym uprawnienia do nakładania surowych kar finansowych.

Z uwagi na szeroką definicję danych osobowych, wiele danych zbieranych przez urządzenia w ramach IoT może podlegać restrykcyjnym zasadom RODO. Problemem jest również brak regulacji dla przedsiębiorców w zakresie dostępu czy wymiany danych o charakterze nieosobowym, ponieważ ogranicza to możliwości wykorzystania tego typu danych w systemach IoT. Przyjęte niedawno Rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej nie odpowiada na wyzwania związane z wykorzystaniem danych anonimowych w IoT. Szczegółowy opis barier regulacyjnych znajduje się w rozdziale 17, strona 102.

Edukacja

System edukacyjny w obecnym kształcie nie zapewnia dostatecznego napływu wykwalifikowanych kadr o specjalności IoT. Nieliczne jak dotąd uczelnie wyższe decydują się na uruchamianie kierunków IoT, oferując je zwykle w programach studiów podyplomowych. Nie jest to skala, która jest w stanie sprostać przewidywanemu zapotrzebowaniu rynkowemu.

Zainteresowani podjęciem studiów kierunkowych IoT mogą skorzystać z następujących, zidentyfikowanych przez Grupę propozycji:

- Akademia WSB – **Sieci komputerowe i Internet Rzeczy** (studia podyplomowe)
- Uniwersytet Ekonomiczny we współpracy z Uniwersytetem Adama Mickiewicza w Poznaniu – **Aplikacje Internetu Rzeczy** (studia II stopnia)
- Społeczna Akademia Nauk – **Internet Rzeczy** (studia podyplomowe)

5 www.crn.pl/artykuly/raporty-i-analizy/internet-of-things-nisza-z-potencjalem?page=1

- WSG w Bydgoszczy – **Przemysłowy Internet Rzeczy** (studia II stopnia)
- Politechnika Poznańska – **Internet Przedmiotów** (specjalność na kierunku Informatyka)
- Akademia Górniczo-Hutnicza w Krakowie – **grupa badawcza IoT**
- Politechnika Wrocławska – **Inżynieria Internetowa** (specjalność na kierunku informatyka)

Doraźnego wsparcia można szukać w kierunkach ogólnych informatycznych (programowanie oraz sprzęt IT), a także matematycznych (modele analityczne, gromadzenie i przetwarzanie danych, sztuczna inteligencja). Jednak wobec dynamicznego rozwoju gospodarki opartej na IoT w Polsce, należy liczyć się z realnym problemem poważnych niedoborów wyspecjalizowanych w tej dziedzinie kadr.

Zagadnienia etyczne

W związku z brakiem przepisów, regulujących kwestie etycznego wykorzystania technologii i systemów IoT, ich dynamiczny rozwój rodzi mnóstwo pytań, na które dziś nie znamy odpowiedzi. Jak rozkłada się odpowiedzialność za skutki działania autonomicznych urządzeń – np. awarii autonomicznego drona dostarczającego przesyłkę, w wyniku której zniszczona została jej zawartość i poszkodowane osoby trzecie – pomiędzy właściciela urządzenia, firmę kurierską, twórcy systemu sterowania oraz operatora i twórcy systemu koordynacji ruchu powietrznego? Kto jest właścicielem danych rejestrowanych przez urządzenia inteligentnego budynku – najemca, wynajmujący, osoby fizyczne których dane dotyczą – i dla jakich celów mogą one być wykorzystywane przed poszczególnych interesariuszy? Jaki poziom niezawodności urządzenia telemedycznego – na przykład dozownika insuliny – jest wymagany dla dopuszczenia go do masowego stosowania w terapii?

Konieczna jest dyskusja nad kwestiami etycznymi, która poprzedziłaby działania prawne. Dodatkowo, etyka dotyka sfery bezpieczeństwa, wskazując potencjalne zagrożenia związane z użytkowaniem systemów IoT. W szczególności, rezultat tej dyskusji będzie miał wpływ na następujące aspekty:

- minimalizacji danych wykorzystywanych przez IoT,
- wprowadzanie komend głosowych (lub innych specyficznych gestów aktywujących urządzenie),
- możliwości dowolnego kasowania danych ze strony użytkownika,
- szyfrowanie danych,
- zarządzanie tożsamością użytkownika.

06
KONTEKST STRATEGICZNY

Polska i Europa dawno już dostrzegły możliwości rozwoju gospodarki w oparciu o technologie IoT.

Komisja Europejska współpracuje z przedstawicielami przemysłu, organizacjami i środowiskiem akademickim, realizując założenia przyjętej w 2015 roku Strategii jednolitego rynku cyfrowego („*Digital Single Market Strategy*"). Strategia wdrażana jest z uwzględnieniem założeń przyjętych w dokumentach roboczych „*Advancing the Internet of Things in Europe*" stanowiącego część wizji „*Digitising European Industry*" oraz „*Liability for emerging digital technologies*".

W ramach **Digital Single Market**, jako priorytetowe zadanie wskazane zostało tworzenie Digital Innovation Hubs (**DIH**) umożliwiających dostęp do nowych technologii małym i średnim przedsiębiorstwom. Są one zebrane w europejskim katalogu DIH-ów, prowadzonym przez Komisję Europejską i zawierającym aż 244 DIH-y z całej Europy, w tym sześć polskich. Każdy z nich w obrębie swoich zainteresowań uwzględnia problematykę Internetu Rzeczy.

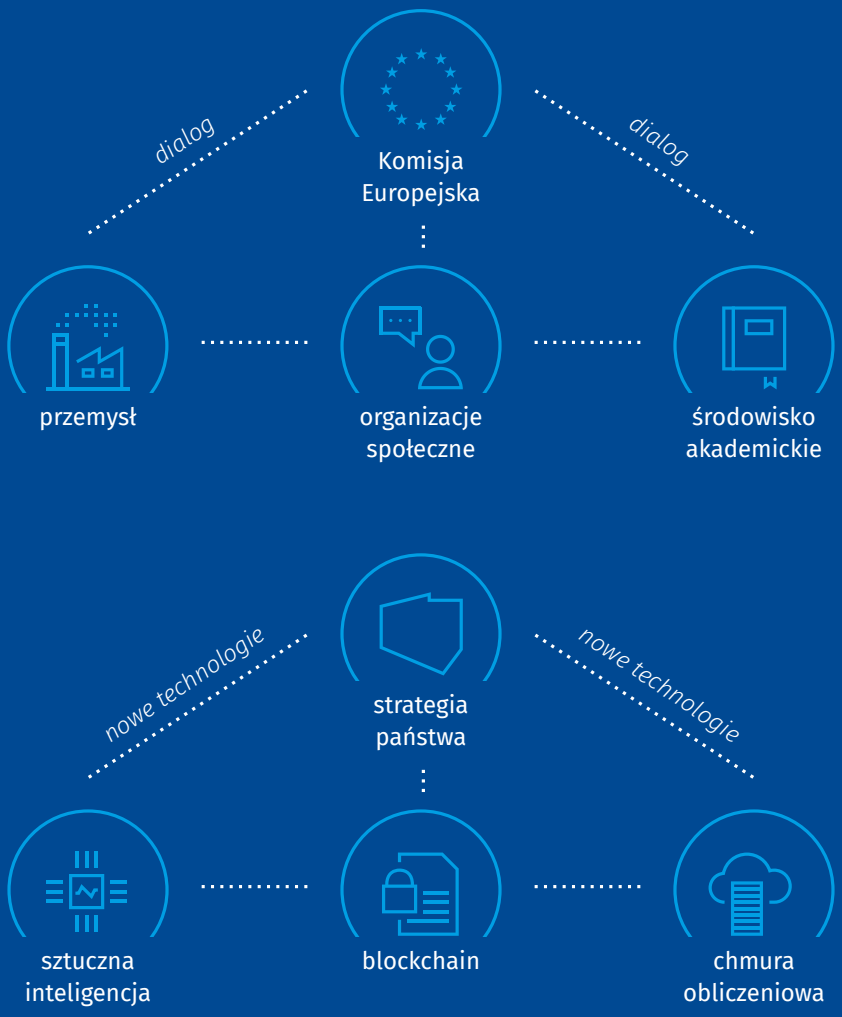
Unia Europejska wspiera również rozwój technologii Internetu przecinek po przeznaczając finansowe na badania i rozwój w ramach programu Horizon 2020. Prawie 500 mln Euro przewidziane w 2014 roku na program, zostanie rozdystrybuowane do 2021. W ramach tego programu powstają między innymi platformy dla współpracy urządzeń i systemów IoT m.in. Inter-IoT, VICINITY czy BIG IoT.

Aktywność Komisji uwidacznia się również w propagowaniu rozwoju IoT na arenie międzyregionalnej. W styczniu 2016 we współpracy z Ministerstwem Przemysłu i Technologii Informacyjnych Chińskiej Republiki Ludowej podpisano „*EU-China Joint White Paper on the Internet of Things*" – wspólny dokument opisujący kilkanaście lat współpracy oraz inicjujący kolejne kroki w zakresie badań i innowacji, kładący szczególny nacisk na kreowanie polityk, wymogów technicznych, międzynarodowych standardów i wymianę informacji w ramach wspólnego rynku.

Polska, wpisując się w globalne trendy, podejmuje szereg inicjatyw mających na celu rozwój gospodarki w kierunku wytyczonym przez światowych liderów. Podejście to wyartykułowane zostało w przyjętej uchwałą Rady Ministrów Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.). Premiuje ona podejście proinnowacyjne, które pozwoli na osiągnięcie wartości dodanej. Internet Rzeczy wprost wymieniony został w niej jako przykład cyfrowej rewolucji technologicznej.

W Strategii wskazano **Krajowe Inteligentne Specjalizacje** (dalej: **KIS**) jako obszary skupienia uwagi, na których powinna być budowana konkurencyjność polskiej gospodarki. Lista specjalizacji jest zarządzana i aktualizowana przez Ministerstwo Przedsiębiorczości i Technologii, ostatnia aktualizacja miała miejsce 1 stycznia 2019 roku. Firmy i rozwiązania wpisujące się w inteligentne specjalizacje mogą liczyć na preferencyjny dostęp do **funduszy wsparcia B+R+I** (dla prac badawczych, rozwojowych i innowacyjności). Technologie IoT znajdziemy w kilu inteligentnych specjalizacjach, m.in.:

- **KIS 1.** Zdrowe społeczeństwo – w zakresie **telemedycyny** i monitorowania stanu zdrowia przy pomocy urządzeń, czujników i akcesoriów;
- **KIS 2.** Innowacyjne technologie, procesy i produkty sektora rolno-spożywczego i leśno-drzewnego – w zakresie teledetekcji, stosowania **technologii LCA** (ang. *Life Cycle Assessment*) oraz wdrażania nowoczesnych systemów monitoringów i wczesnego ostrzegania;
- **KIS 4.** Wysokosprawne, niskoemisyjne i zintegrowane układy wytwarzania, magazynowania, przesyłu i dystrybucji energii – w zakresie inteligentnych sieci elektroenergetycznych (ang. *Smart Grids*);
- **KIS 9.** Sensory (w tym biosensory) i inteligentne sieci sensorowe – w zakresie budowy i rozwoju sieci sensorowych opartych w szczególności o **komunikację M2M**;
- **KIS 11.** Elektronika drukowana, organiczna i elastyczna – w zakresie druku inteligentnych obiektów (ang. *Smart Objects*).



Programy Pierwszej Prędkości przewidziane w Strategii obejmują likwidację barier rozwojowych, w tym legislacyjnych, organizacyjnych i instytucjonalnych, zidentyfikowanych również przez Grupę ds. Internetu Rzeczy w niniejszym raporcie.

Strategia państwa w obszarze wsparcia innowacji opartych na IoT uwzględnia także regulacje dotyczące przetwarzania danych osobowych jak i nieosobowych, a także dostrzega potencjał wykorzystania danych maszynowych generowanych w dużej mierze przez samych użytkowników. W dobie nowych technologii wartość danych jest nie do przecenienia, ale ich szerokiej dostępności towarzyszyć muszą wysokie standardy ochrony. Dopiero zapewnienie tych dwóch elementów pozwoli na pełne rozwinięcie potencjału gospodarczego bez szkody dla prywatności osób fizycznych oraz wartości intelektualnej przedsiębiorstw.

Rząd zdaje sobie sprawę, że realny potencjał rozwojowy kraju zależy od holistycznego podejścia do rozwoju nowych technologii, które mają okazję uzupełniać, udoskonalać i kooperować z innymi zdobyczami techniki, takimi jak **sztuczna inteligencja**, **blockchain**, rozwiązania oparte o **chmurę obliczeniową**, czy sieć 5G.

Podwaliny pod dynamiczny rozwój Internetu Rzeczy kładą liczne programy, takie jak Strategia 5G dla Polski w Ministerstwie Cyfryzacji, czy aktywność Grupy Roboczej do spraw Sztucznej Inteligencji. Wspomniane technologie mogą funkcjonować niezależnie, ale dopiero połączone miedzy sobą w większe systemy i organizmy gospodarcze ukazują niesiony przez siebie potencjał przyczyniający się zarówno do zwiększenia komfortu obywatela, jak i wartości sektora przedsiębiorstw.

Nie mniej istotna jest budowa sprzyjających innowacyjności form prawnych prowadzenia działalności gospodarczej. W tym celu podjęto prace nad stworzeniem nowego rodzaju spółki – Prostej Spółki Akcyjnej, mającej charakter spółki prywatnej, z obniżonymi wymogami kapitałowymi, uproszczonym trybem zakładania, jak i likwidacji. Jest to rozwiązanie dedykowane **startup-om**, w szczególności z branży nowych technologii. Dzięki oderwaniu wartości akcji od kapitału akcyjnego spółki, akcjonariusze wzbogacający podmiot o zasoby intelektualne, będą mogli swoim głosem stanowić przeciwwagę dla akcjonariuszy wnoszących kapitał w formie wkładu pieniężnego lub aportu.

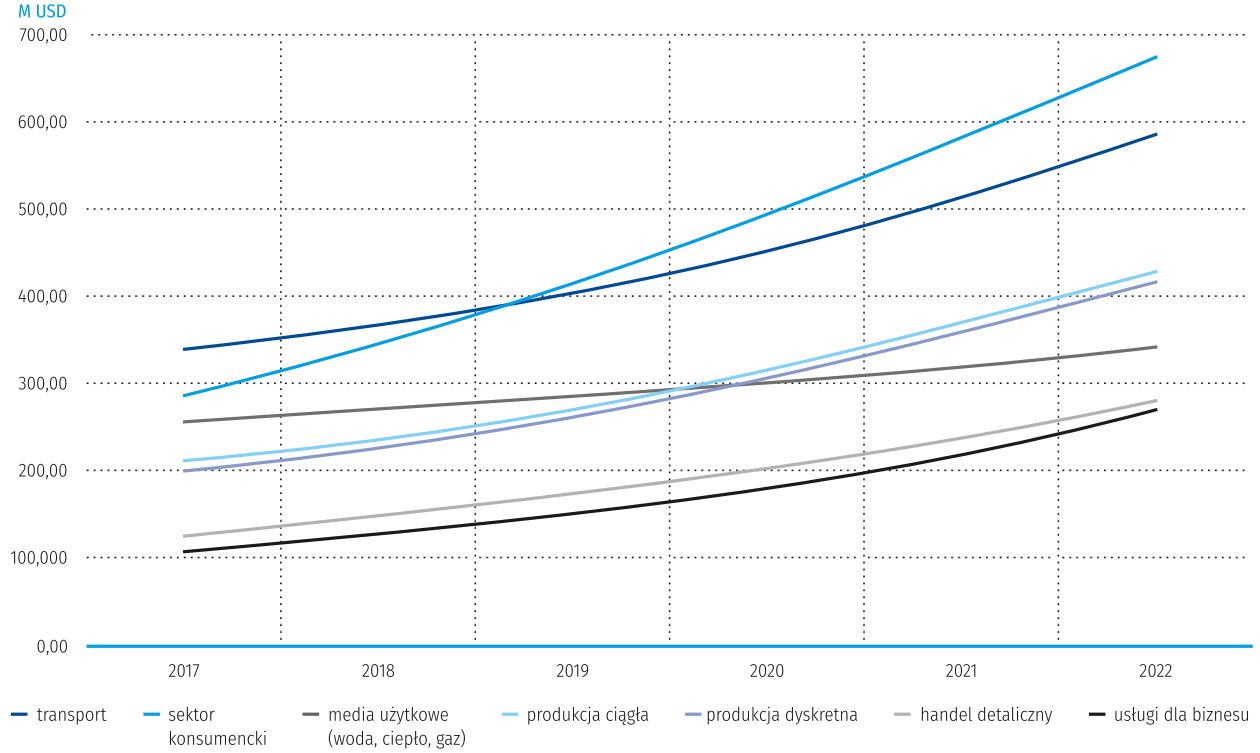
07

BRANŻE O SZCZEGÓLNYM POTENCJALE ROZWOJU W POLSCE W OPARCIU O IoT

Technologia IoT ma charakter horyzontalny. To oznacza, że może być wykorzystywana w wielu różnych branżach i rozwiązaniach biznesowych. Dodatkowo, w ramach każdej branży systemy IoT mogą występować na różnych etapach łańcucha dostaw, tworząc ekosystemy rozwiązań, przenikających poszczególne segmenty rynku. Niemniej niektóre branże będą znacznie silniej uzależnione od systemów Internetu Rzeczy i na nich powinny skupić się działania wspierające rozwój rynku IoT.

Według danych dotyczących rynku globalnego, liderami wzrostów i wolumenu wydatków w obszarze IoT są: rynek konsumencki, branża logistyczna i transportowa oraz przemysł. Ze wszystkich branż, które najbardziej inwestują w technologię IoT, jedynie branża handlowa, nie podjęła dotychczas wyzwania szerokiej adopcji systemów IoT (pomimo tego, że jest na 6 miejscu pod względem wydatków na tę technologię). Jest to zapewne związane z brakiem wystarczająco przekonujących scenariuszy monetyzacji tych inwestycji.

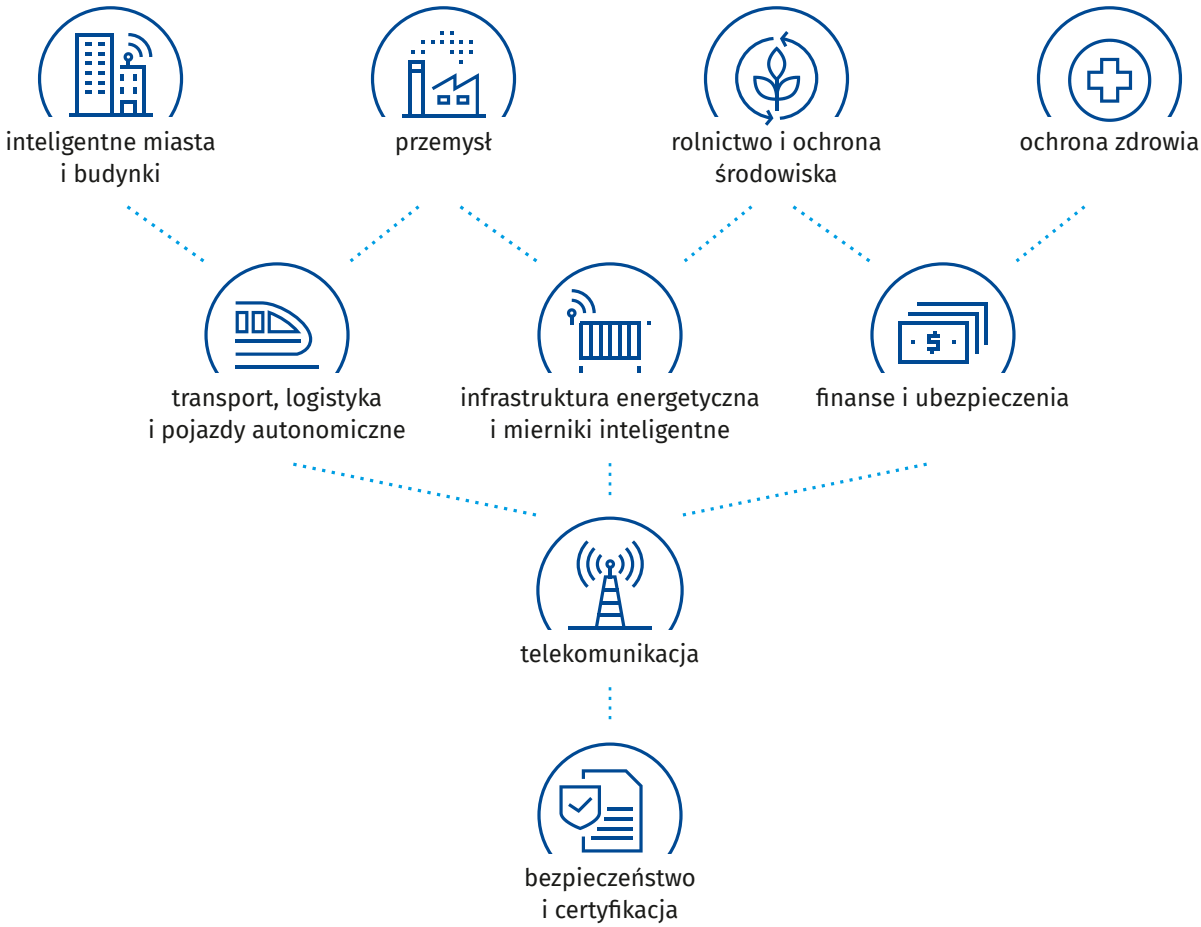
Wydatki na IoT w poszczególnych branżach



Źródło: IDC Worldwide Semiannual Internet of Things wydatki w poszczególnych branżach, czerwiec 2018

Sektor	2017	2018	2019	2020	2021	2022
sektor konsumencki	287,82	345,15	412,49	492,50	581,47	677,56
transport	338,89	367,43	404,24	450,29	511,36	585,19
produkcja ciągła	208,53	234,85	270,34	313,94	366,55	428,96
media użytkowe	258,37	269,87	284,29	301,29	320,80	343,64
produkcja dyskretna	196,39	224,62	260,48	307,40	356,96	421,32
handel detaliczny	126,51	146,98	173,14	201,85	237,06	278,99
usługi dla biznesu	106,59	124,35	149,93	178,61	214,96	269,67
władze krajowe/lokalne	72,77	81,56	91,63	104,31	119,92	140,02
usługi dla ludności	56,20	64,91	77,35	95,89	118,25	149,62
sprzedaż hurtowa	56,10	64,31	77,31	92,78	108,58	127,19
władze federalne/centralne	58,02	66,05	76,87	89,34	101,70	118,30
ochrona zdrowia	62,24	66,79	73,24	80,48	90,66	104,90
edukacja	29,81	34,97	43,76	54,12	65,10	77,55
budownictwo	31,78	35,80	41,02	48,50	56,55	65,93
telekomunikacja	28,07	31,89	36,94	43,24	49,95	57,90
media	26,38	29,93	34,81	42,07	49,54	58,62
przemysł wydobywczy	17,04	19,69	22,80	26,58	31,09	36,36
ubezpieczenia	8,65	10,60	13,33	17,43	22,13	28,44
papiery wartościowe i usługi inwestycyjne	6,56	7,21	8,19	9,24	10,72	12,33
bankowość	3,44	4,16	5,04	5,93	7,05	8,14
Suma końcowa	**1980,14**	**2231,10**	**2557,18**	**2955,78**	**3420,39**	**3991,66**

Na podstawie opisanych powyżej trendów, a także biorąc pod uwagę strukturę polskiej gospodarki, Grupa dokonała wyboru 9 najważniejszych branż z punktu widzenia wolumenu korzyści wynikających z możliwości zastosowania IoT w Polsce. Należą do nich:



08

BEZPIECZEŃSTWO I CERTYFIKACJA

IoT bez cyberbezpieczeństwa stanowi większe zagrożenie dla państwa niż rezygnacja z użycia IoT

AUTORZY:
ALEKSANDER P. CZARNOWSKI, AVET INFORMATION AND NETWORK SECURITY – LIDER PODGRUPY
ANDRZEJ KARPIŃSKI, ORANGE POLSKA
KONRAD KOWALCZUK, MGK.NET.PL
ANDRZEJ PIOTROWSKI, UTC FIRE & SECURITY POLSKA
RAFAŁ RADAWIEC, POLITECHNIKA WROCŁAWSKA
MARIOLA WIĘCKOWSKA, LEXDIGITAL

Ogólna charakterystyka

Ze względu na upowszechniający się zasięg IoT oraz masowe przetwarzanie danych mających znaczenie dla gospodarki, a także obronności kraju, IoT nie może istnieć bez cyberbezpieczeństwa. Brak adekwatnych regulacji prawnych oraz certyfikacyjnych spowoduje, że Polska straci istotny element przewagi zarówno w kontekście gospodarczym, ochrony obywateli, jak i innowacyjnym.

Innowacje i dynamiczny rozwój technologiczny, globalizacja oraz coraz krótszy czas wprowadzania produktów na rynek powodują, że producenci, importerzy i sprzedawcy detaliczni produktów IoT stoją w obliczu szeregu wyzwań. Surowe wymagania rynku dotyczące niezawodności i wydajności produktów, a także zmieniające się regulacje prawne, wzmagają poczucie presji.

Chcąc wpływać na zachowania konsumenckie trzeba zwracać uwagę na istnienie przepisów i wymagań z nimi związanych oraz na prezentowaniu zależności pomiędzy certyfikacją produktu, a jego kryteriami bezpieczeństwa. Dzięki temu, w każdym miejscu na świecie nabywca rozwiązania ma świadomość ochrony swoich praw i przestrzegania zasad. Certyfikacja jest najbardziej wiarygodnym sposobem zapewnienia nabywcy o odpowiednim standardzie wyrobów i usług.

Bezpieczeństwo jest krytycznym elementem jakości produktu. Poziom bezpieczeństwa trudno poddaje się prostej ocenie, dlatego należy wypracować standardy i najlepsze praktyki w tym zakresie. Powyższe elementy muszą być kompatybilne z istniejącymi już międzynarodowymi i europejskimi standardami, jednakże gwarantując ochronę interesów Polski. Z drugiej strony zbyt silne uregulowanie może ograniczyć innowacyjność oraz niebezpiecznie zawyżyć próg wejścia dla nowych rozwiązań, co przyniesie negatywne skutki gospodarcze długofalowo dla rodzimych przedsiębiorców. Bezpieczeństwo należy postrzegać jako podstawową funkcję świata IoT. Bez spełnienia wymogów bezpieczeństwa, stosowania standardów i dobrych praktyk, świat IoT stanowi samodzielnie większe zagrożenie, niż w przypadku rezygnacji z tego typu technologii. Bezpieczeństwo to zatem warunek niezbędny dla rozwoju IoT. Natomiast bez adekwatnej certyfikacji produktów IoT, nie można zapewnić odpowiedniego poziomu bezpieczeństwa.

Bezpieczeństwo w systemach IoT możemy podzielić na kilka podkategorii, takich jak:

- **bezpieczeństwo produktu** z punktu widzenia norm dotyczących higieny, toksyczności, funkcjonalności, ergonomii itp., które gwarantują bezpieczne użytkowanie produktu;
- **cyberbezpieczeństwo produktu**, rozumiane jako odpowiedni poziom wykonania produktu, oraz wyposażenia go w narzędzia i mechanizmy przeciwdziałające zagrożeniom teleinformatycznym;
- **bezpieczeństwo danych** przetwarzanych przez produkt, lub ekosystem informacji dotyczących otoczenia, zarówno osobowych, jak i technicznych (np. **telemetrycznych**, nieosobowych);
- **bezpieczeństwo fizyczne**, dotyczące wpływu technologii IoT i jej zastosowania na świat fizyczny (oddziaływanie bezpośrednie i wpływ świata IoT na codzienne życie obywateli np. funkcje blokady drzwi, skrętu auta autonomicznego, kontroli przepływu w wodociągach, czy prawidłowe działanie urządzenia telemedycznego takiego jak stymulator serca);
- **bezpieczeństwo prawne i regulacyjne**, rozumiane jako spełnienie przez urządzenia IoT norm prawnych dotyczących np. dopuszczalności przetwarzania przez nie określonych informacji;
- **bezpieczeństwo narodowe, militarne**, rozumiane jako potencjalna możliwość wykorzystania infrastruktury IoT m.in. do szpiegowania poprzez zbieranie informacji, nieautoryzowanego wykorzystania metadanych, spowodowania celowego unieruchomienia ważnych komponentów infrastruktury krytycznej czy awarii masowej, możliwości wykorzystania narzędzi IoT jako bezpośredniego narzędzia do ataku lub spowodowania katastrofy (np. dron czy **pojazd autonomiczny**).

Certyfikacja w przypadku rozwiązań IoT powinna dotyczyć:

- Potwierdzenia spełnienia przez urządzenie norm krajowych i międzynarodowych w zakresie typowym dla każdego sprzętu danej klasy/kategorii – np. potwierdzenie Instytutu Matki i Dziecka dla produktów dla dzieci, potwierdzenie w zakresie norm energetycznych, dopuszczalnego poziomu hałasu, zanieczyszczeń, rodzaju użytego materiału, zakresu temperatur pracy itd.
- Wskazanie klasy jakości urządzeń, poprzez określenie dokładności pomiaru czy precyzji działania urządzenia, warunków, przy których parametry zostaną zachowane, oraz czasu, przez który można założyć utrzymanie zmierzonych parametrów. Jest to o tyle istotne, że oczekiwana precyzja wprost zależy od konkretnego zastosowania, i użytkownik musi mieć precyzyjną informację, z jakiej klasy urządzeniem pracuje. Klasy te powinny zostać poddane normalizacji – warto stworzyć nazwany katalog parametrów urządzeń IoT, wraz z klasami dokładności, podobnie jak ma to miejsce np. w oznaczeniach podzespołów elektronicznych (np. 10 Ohm z dokładnością 10%, gwarantowane przez 10 lat, pod warunkiem użytkowania w temperaturze x-y).
- Certyfikacja części komunikacyjnej, na okoliczność zgodności z ogólnie przyjętymi standardami komunikacji IoT – stopień wypełnienia definicji protokołów, **interfejsów aplikacyjnych** (ang. *API – Application Programming Interface*), itd.

- Certyfikacja pod kątem cyberbezpieczeństwa – na dziś brak jednego ogólnie przyjętego standardu międzynarodowego dla IoT. Najbliższe w tym zakresie są opracowania ENISA oraz Common Criteria. Prace na laboratorium certyfikacyjnym opartym na Common Criteria w Polsce są w toku.

W zakresie certyfikacji niezbędne wydaje się stworzenie krajowej jednostki certyfikacyjnej lub powierzenia zadań związanych z certyfikacją istniejącej instytucji/laboratorium. Jednocześnie mechanizm akredytacji i certyfikacji musi być zgodny z mechanizmem dostępnym w ramach RODO. Grupa widzi potencjał biznesowy w istnieniu sprawnej, krajowej jednostki certyfikacyjnej, tak w zakresie wspierania rynku krajowego producentów IoT, w udziale Polski w budowaniu międzynarodowych norm i standardów, jak i możliwości prowadzenia komercyjnych testów przez krajową jednostkę certyfikacyjną, zamiast certyfikacji urządzeń poza granicami kraju.

Korzyści z certyfikacji dla przemysłu:

- certyfikacja jest narzędziem marketingowym i sprzedażowym otwierającym lokalne i międzynarodowe rynki zbytu – co więcej zgodny system certyfikacji z międzynarodowymi normami gwarantuje możliwość lokalnej certyfikacji w sposób akceptowalny globalnie;

- certyfikacja jest niezbędnym narzędziem w procesie podejmowania decyzji oraz przy zarządzaniu ryzykiem. Organizacje mogą oszczędzić czas i pieniądze poprzez wybór składników certyfikacji, zadbać aby ich produkt mógł być rozpoznawalny (w celu uzyskania zgodności ze światowymi normami);

- certyfikacja zapewnia precyzyjne pomiary i badania przeprowadzane zgodnie z najlepszą praktyką, ogranicza liczbę wyrobów wadliwych, obniża koszty kontroli i produkcji oraz umożliwia wdrażanie innowacyjnych rozwiązań (w tym zakresie certyfikacja może wydłużyć proces dostarczenia na rynek innowacji);

- certyfikacja zmniejsza ryzyko w relacjach biznesowych;

- certyfikacja pozwala na ograniczenie produktów niskiej jakości podszywających się pod czołowego producenta oraz redukuje liczbę podróbek.

Korzyści z certyfikacji dla konsumentów:

- dzięki certyfikacji możliwe są wiarygodne i precyzyjne wyniki analiz oraz badań w obszarach związanych z bezpieczeństwem, zdrowiem i środowiskiem (np. analizy medyczne, badania mechaniczne, badania chemiczne);

- jednostki certyfikacyjne dostarczają wiarygodnych informacji, na podstawie których mogą być podjęte decyzje np. w zakresie cyberbezpieczeństwa, ochrony środowiska (**RoHS** ang. *Restriction of Hazardous Substances*) czy w ramach świadectwa jakości CE;

- certyfikacja przyczynia się do likwidacji barier w handlu poprzez wzajemne uznawanie procedur oceny zgodności (swobodny handel międzynarodowy jest stymulatorem wzrostu ekonomicznego).

Korzyści z certyfikacji dla państwa polskiego:

- certyfikacja daje możliwość stymulowania rynku krajowego;

- certyfikacja otwiera możliwości awansu do pozycji gracza globalnego na danym rynku;

- certyfikacja podnosi gwarancję bezpieczeństwa produktów i ekosystemu z punktu widzenia zdarzeń o charakterze indywidualnym i masowym.

Perspektywa rozwoju branży

Przewiduje się, że w ciągu najbliższych lat, ilość ruchu autonomicznego wygenerowanego przez IoT w sieci przekroczy ilość ruchu wprost generowanego przez użytkowników. W wybranych kategoriach, to zjawisko już wystąpiło – przykładem jest poczta elektroniczna, gdzie blisko 90% wiadomości w sieci jest generowana przez automaty. Taki gwałtowny wzrost ruchu i liczby urządzeń podłączonych do sieci, przełoży się wprost na skalę i rodzaj zagrożeń związanych z bezpieczeństwem. Już dziś przykładowo największe sieci (**botnety** – sieci składające się z wielu zainfekowanych szkodliwym oprogramowaniem komputerów, od ang. *Robot i Net*) używane do ataków kończących się sukcesem na inne systemy, a czasem całe państwa, są budowane z wykorzystaniem urządzeń IoT.

Internet Rzeczy to trend, którego producenci nie mogą zignorować. Oczekuje się, że IoT połączy do 2020 roku aż 28 miliardów urządzeń. Urządzenia są coraz częściej wyposażone w połączenie z Internetem i zmieniają się w elementy systemów IoT: od smart TV, **asystentów cyfrowych**, inteligentnych zabawek, **trackerów** fitness i podłączonych do sieci urządzeń domowych, aż po kompletny inteligentny dom. Daje to wiele korzyści: większą wygodę, większe bezpieczeństwo i mniejsze zużycie energii. Konsumenci są gotowi zapłacić za wygodę podłączonych urządzeń, które mogą poprawić sposób ich pracy i jakość życia.

W przypadku urządzeń IoT przeznaczonych do użycia w pobliżu ciała ludzkiego, takich jak akcesoria do noszenia, potrzebne będą również **testy SAR** oraz **wymogi IEEE/FCC**. Chociaż interoperacyjność jest niewidoczna dla konsumenta, ważne jest, aby producenci upewnili się, że ich urządzenie IoT może komunikować się płynnie z innymi urządzeniami. Każdy producent powinien zadać sobie pytanie, czy jego produkt lub usługa IoT spełnia wysokie wymagania przepisów dotyczących ochrony danych i bezpieczeństwa danych, a także czy

uwzględnia oczekiwania konsumentów dotyczące ich prywatności.

Polskie Centrum Akredytacji jest krajową jednostką akredytującą upoważnioną do akredytacji jednostek certyfikujących (oceniających) zgodność na podstawie norm międzynarodowych i polskich. Polska posiada 50 akredytowanych jednostek badawczych.

Poniżej prezentujemy przykład listy atrybutów, które mogą być wykorzystane do stworzenia regulacji dotyczącej spójnej certyfikacji dla różnych urządzeń IoT.

Przykładowa klasyfikacja IoT

1 IoT JAKO SYSTEM URZĄDZEŃ
- 1.1 Auto konfiguracja (Auto-configuration)
- 1.2 Zarządzanie komponentami i Funkcje Systemu
- 1.3 System Rozproszony
- 1.4 Połączenie (sieciowe) urządzeń
- 1.5 Zarządzanie urządzeniami i dostępem do nich
- 1.6 Synchronizacja działań
- 1.7 Jakość dopasowania (protokoły/standardy)
- 1.8 *Licencje/Subskrypcje/Model działania

2 IoT JAKO SYSTEM USŁUG
- 2.1 Opis usługi wg. dokumentacji (Content-Awareness)
- 2.2 Działanie usługi wg schematu (Context-Awareness)
- 2.3 Dostępność (jako atrybut ISO 27001)

3 IoT JAKO KOMPONENT
- 3.1 Zgodność z konwencjami
- 3.2 Wykrywalność
- 3.3 Modularność
- 3.4 Możliwość dostępu sieciowego
- 3.5 Dostępność
- 3.6 Unikalny numer/nazwa

4 KOMPATYBILNOŚĆ
- 4.1 Wsparcie techniczne
- 4.2 Wsteczna kompatybilność

5 UŻYTECZNOŚĆ
- 5.1 Łatwość obsługi (zgodna ze standardami)
- 5.2 Operacyjność

6 SPECJALISTYCZNE
- 6.1 Dokładność (dla urządzeń pomiarowych)
- 6.2 Wytrzymałość (w rozumieniu ograniczeń działania)
- 6.3 Żywotność (dla urządzeń z baterią/ czujnikiem)

7 BEZPIECZEŃSTWO
- 7.1 Dostępność
- 7.2 Poufność
- 7.3 Integralność
- 7.4 Bezpieczeństwo (testy penetracyjne/fuzz testing)

8 ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI
- 8.1 RODO
- 8.2 PSD2 / NIS
- 8.3 Prawa narodowe
- 8.4 Inne akty prawne

9 INNE ATRYBUTY
- 9.1 Wiarygodność.
- 9.2 Możliwość zapisu i odczytu w innych systemach i różnorodność wykorzystania danych (prawne aspekty)
- 9.3 Zgodność z przepisami UE

Źródło: The Singapore Economic Development Board, IoT Proposal Draft, 2017

Zakres możliwego wykorzystania IoT

Zapewnienie bezpieczeństwa, poprzez stosowanie odpowiednich norm, standardów i certyfikacji jest możliwe, ale wymaga edukacji społeczeństwa i podniesienia świadomości w zakresie tego, gdzie IoT jest wykorzystywane. Sfery życia społeczno-gospodarczego, które posiadają największy potencjał do tworzenia wartości poprzez wykorzystanie koncepcji Internetu Rzeczy to[1]:

- ludzie,
- mieszkanie,
- handel detaliczny,
- biura,
- fabryki,
- miejsca pracy/place budowy (np. miejsca wydobycia ropy naftowej),
- pojazdy,
- miasta,
- obszary zewnętrzne), tj. obszary znajdujące się pomiędzy środowiskami zurbanizowanymi.

Jednocześnie potencjalny wpływ ekonomiczny Internetu Rzeczy będzie mocno różnić się w odniesieniu do poszczególnych sfer jego oddziaływania. Według prognoz firmy McKinsey do roku 2025 największy wpływ zostanie odnotowany w sferze związanej z fabrykami (1,2–3,7 biliona USD), natomiast najmniejszy w sferze biurowej (70–150 mld USD)[2]. W powyższym kontekście zauważyć też należy, że jedynie około 10% wartości finansowej czerpanej przez organizacje z Internetu Rzeczy pochodzić będzie z „rzeczy" jako takich, natomiast pozostała część wynikać będzie z tego, w jaki sposób podłączone zostaną one do Internetu i w jakim celu[3]. Stąd też niezwykle istotne jest, jak organizacje i państwa „konstruować" będą swoje ekosystemy IoT.

Bariery

W toku prac Grupa zidentyfikowała następujące bariery dla branży:

- Brak krajowego schematu certyfikacji IoT wraz ze schematem akredytacji krajowych jednostek certyfikacyjnych, który byłby zgodny z Common Criteria i mechanizmem akredytowanych kodeksów postępowania, opisanym w sekcji 5 (Kodeksy postępowania i certyfikacja) RODO, a w szczególności w art. 40, 41, 42, i 43 RODO.

- Brak uwzględnienia zjawiska IoT w przepisach prawa dotyczących bezpieczeństwa, w szczególności w zakresie Prawa Telekomunikacyjnego czy ustawie o Krajowym Systemie Cyberbezpieczeństwa; brak zdefiniowania IoT jako rynku przez UKE;

- Brak jednoznacznych rozwiązań legislacyjnych regulujących i adresujących problemy IoT w zakresie cyberbezpieczeństwa;

- Problemy z zagwarantowaniem interoperacyjności, otwartości i dostępności.

Jak pokazują wczesne i stosunkowo proste wdrożenia w obszarze IoT, skala potencjalnych problemów związanych z tymi kwestiami może być znacząca[4].

Jeśli chodzi o zagadnienia związane z zapewnieniem interoperacyjności, to według ocen firmy konsultingowej McKinsey jest to krytyczny aspekt w kontekście przyszłości i rozwoju systemów Internetu Rzeczy. Wiążą się one z wypracowaniem otwartych standardów we wszystkich obszarach i na wszystkich poziomach, tak aby możliwa była płynna i bezproblemowa współpraca oraz komunikowanie się urządzeń pochodzących od różnych dostawców i budowanie na ich bazie ekosystemów IoT.

Według ocen McKinsey'a bez zapewnienia interoperacyjności co najmniej 40% potencjalnych korzyści związanych z Internetem Rzeczy nie zostanie osiągnięte[5]. Jednocześnie wskazać można cały szereg wyzwań natury pozatechnicznej. W związku z tym, że w systemach Internetu Rzeczy wartość w znacznym stopniu tworzona jest na bazie pozyskiwanych, przesyłanych, przetwarzanych i analizowanych danych[6], kwestie związane z nimi stanowią jeden z kluczowych aspektów mogących wyrastać na bariery rozwojowe tej koncepcji lub też stymulować jej rozwój.

Jednocześnie bariery czy też wyzwania mogące przekształcić się w stymulatory, występują na różnych poziomach, tj.:

- globalnym – np. globalne tendencje cenowe komponentów infrastruktury IoT, globalne standardy,

- regionalnym – np. unijne standardy i regulacje dotyczących różnych aspektów Internetu Rzeczy,

- krajowym – np. regulacje i standardy na rynkach poszczególnych państw,

- sektorowym – np. branżowe regulacje i standardy.

1 McKinsey Global Institute, The Internet of Things: Mapping the value beyond the hype, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
2 Ibidem
3 Bauer et al. 2015, McKinsey 2014
4 por. Blaich 2016
5 McKinsey 2015
6 Heppelmann, Porter 2014, ss. 64–88.

Propozycje działań rządu

Bezpieczeństwo jest kluczowym elementem ekosystemu IoT. Ważne jest posiadanie odpowiednich narzędzi do jego zapewnienia, oceny i certyfikacji. Narzędzia muszą mieć odpowiednie umocowanie prawne, podlegać standardom/spełniać standardy i najlepsze praktyki. Interoperacyjność jest kluczowym wymogiem nie tylko dla zarządzania cyberbezpieczeństwem, ale także dla innych biznesowych zastosowań. W związku z tym, rekomendujemy następujące działania:

- Stworzenie jednego, wspólnego słownika pojęć IoT, który będzie używany w całej legislacji, a także w dokumentach normatywnych, najlepszych praktykach i materiałach edukacyjnych. Pozwoli to zmniejszyć istniejącą niepewność co do konkretnych sformułowań wykorzystywanych w dokumentach oraz przyspieszy proces standaryzacji systemów IoT.

- Wypracowanie norm w zakresie cyberbezpieczeństwa, interoperacyjności i standaryzacji oraz metod ich certyfikacji. Normy muszą być dostosowane do potrzeb rynku. Należy wprowadzić różne progi certyfikacji, w zależności od przewidywanego czasu życia oraz zastosowań rozwiązań IoT.

- Konieczność przygotowania systemu prawnego do ekosystemu IoT uwzględniając takie aspekty jak: Krajowy System Cyberbezpieczeństwa, RODO, Prawo Telekomunikacyjne, PSD2 czy ePrivacy.

- Konieczne jest wprowadzenie przepisów, regulujących sposób jednoznaczny prawo do wykorzystywania zgromadzonych danych oraz miejsca ich przechowywania.

- Należy przywiązać dużą wagę do aspektów związanych z przetwarzaniem danych nieosobowych, i związanych z nimi metadanych (telemetria oraz związane z nią trendy, wgląd w opisywane nią zdarzenia), a także możliwe połączenie ich z danymi osobowymi.

- Rozpatrywanie bezpieczeństwa całościowo w toku prowadzonych działań – nie wystarczy zabezpieczenie urządzeń końcowych, czy samo zapewnienie globalnych narzędzi nadzoru. Ekosystem IoT powinien być budowany w oparciu o zasadę security-by-design (bezpieczeństwo jest integralnym elementem projektu zgodnie z art. 25 RODO) oraz security-in-deph (zabezpieczenia są adekwatne do roli urządzenia i dla każdego zagrożenia jest więcej niż jedno zabezpieczenie), a także o pogłębianie świadomości samych użytkowników.

- Wprowadzenie odpowiedzialności producentów i integratorów urządzeń, a także systemów IoT w zakresie zapewnienia bezpieczeństwa oraz zdefiniowanie odpowiedzialności w przypadku wycofania produktu, bankructwa lub likwidacji producenta.

- Utworzenie krajowych centrów certyfikacji. Trzy rodzaje certyfikacji uznane w prawie wiążą się z wysokim kosztem i długim okresem oczekiwania. To stanowi wyzwanie i barierę dla startup-ów. Konieczna jest zmiana podejścia w europejskich Common Criteria na bardziej elastyczne tzn. nieniosące ryzyka utraty certyfikatu w przypadku ulepszenia rozwiązania.

09

FINANSE I UBEZPIECZENIA

Dla sektora finansowego i ubezpieczeniowego zapewnienie stałego dostępu do strumieni danych IoT jest jednym z najpoważniejszych wyzwań. Sprostanie mu będzie decydować o porażce lub sukcesie w biznesie.

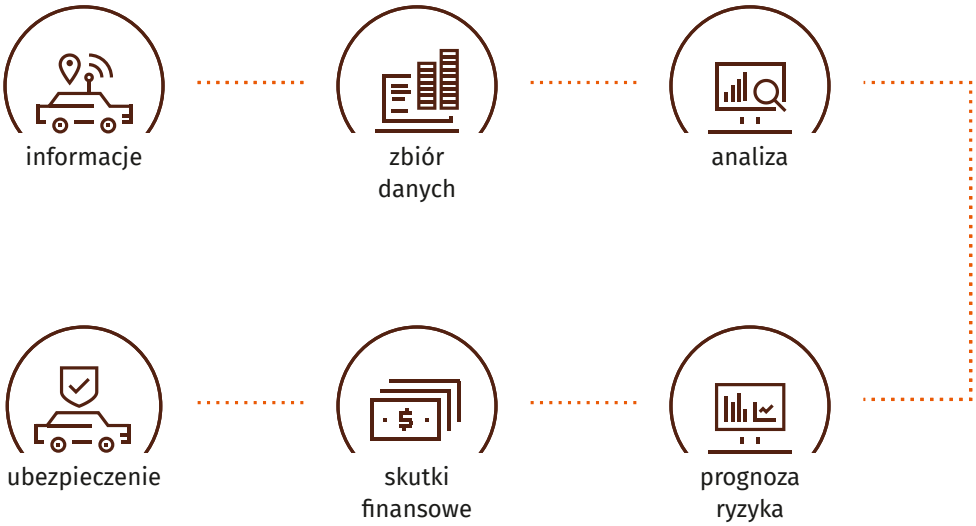
AUTORZY:
MARCIN WOLSKI, STARTUP BILLON GROUP – LIDER PODGRUPY
PIOTR JAN BROZOWSKI, KRAJOWA IZBA DORADCÓW PODATKOWYCH
TOMASZ KLUWAK, KRAJOWA IZBA DORADCÓW PODATKOWYCH
PRZEMYSŁAW KRZYWANIA, BKF MYJNIE BEZDOTYKOWE
MARIUSZ KUNA, POLSKA IZBA UBEZPIECZEŃ
MICHAŁ KWIECIŃSKI, PLATFORMA DETALISTÓW
MACIEJ LECIEJEWSKI, REGENT INSURANCE BROKERS (POLSKA)

Ogólna charakterystyka branży

Branża finansowo-ubezpieczeniowa reprezentowana jest przez podmioty, świadczące usługi płatnicze, zakłady ubezpieczeń, instytucje rozliczeniowe oraz firmy świadczące usługi bankowe.

Sektor finansowy dostrzegł potencjał IoT stosunkowo niedawno wraz z pojawieniem się możliwości wykorzystania komercyjnych rozwiązań opartych o zbieranie informacji z czujników danych.

Procesy w sektorze finansowym i ubezpieczeniowym są oparte o informacje oraz zachodzące między nimi relacje. Analiza zbiorów danych pozwala na prognozowanie elementów ryzyk i pomaga w szacowaniu skutków finansowych.



Mówiąc o IoT w kontekście finansów i ubezpieczeń należy pamiętać, iż zbieranie i przesyłanie danych będzie praktycznie zawsze powiązane z płatnościami za usługi. Oznacza to, iż element płatności, mikropłatności oraz zasad opodatkowania tego typu działań powinien być uwzględniony w strategii państwa w zakresie wykorzystania technologii IoT.

Stanie się on integralną częścią usług IoT, dlatego powinien być traktowany jako element obowiązkowy przy projektowaniu wszelkiego rodzaju produktów i usług.

Nieodłącznym aspektem warunkującym stan branży jest obszar regulacyjny, który ulegał znaczącym modyfikacjom w ostatnich latach. Jednym z najważniejszych aktów prawnych dla sektora finansowo-ubezpieczeniowego działającego w Unii Europejskiej jest Dyrektywa **PSD2**, która otwiera nowe możliwości dla urządzeń IoT.

Perspektywa rozwoju branży

Obszar IoT jest postrzegany jako szansa dla branży ubezpieczeniowej oraz klientów zakładów ubezpieczeń.

Ubezpieczyciele prognozują, iż nowe rodzaje danych oraz ich wysoka dostępność może istotnie wpłynąć na kształt usług i produktów ubezpieczeniowych zarówno od strony samych ubezpieczycieli, jak i klientów zakładów ubezpieczeń. IoT otwiera nową perspektywę patrzenia na te dane.

IoT w sektorze ubezpieczeń w pierwszej kolejności dotyczyć będzie ubezpieczeń majątkowych.

Czujniki pozwolą na kontrolowanie stanu i zmian zachodzących w przedmiotach stanowiących przedmiot ubezpieczeń i sprawią, iż:

- poszerzony zostanie katalog przedmiotów podlegających ubezpieczeniu. Umożliwi to ubezpieczenie przedmiotów oraz ich elementów, które dotychczas nie mogły zostać objęte ubezpieczeniem z uwagi na brak mechanizmów weryfikacji informacji o ich stanie i zagrożeniach. Idea opomiarowania różnych elementów przedmiotów codziennego użytku stwarza szansę na oferowanie ubezpieczeń dla nowych produktów np. ubezpieczenia rowerów, pojazdów elektrycznych;
- uporządkowane zostaną informacje o przedmiotach ubezpieczenia – informacje będą pochodzić bezpośrednio z przedmiotu ubezpieczenia, a nie będą wynikiem ich przetworzenia i klasyfikacji przez inny podmiot;
- zwiększy się precyzja szacowania prawdopodobieństwa wystąpienia zdarzeń i ryzyk jakie one generują – na podstawie stale zwiększającej się puli pomiaru;
- możliwe będzie oferowanie nowych produktów i usług, opracowanych na podstawie danych pozyskanych z nowych źródeł. Dane z IoT pozwolą na wprowadzenie działań proaktywnych po wystąpieniu zdarzenia. Przyjmujemy, iż dzięki danym z czujników, zakłady ubezpieczeń w czasie rzeczywistym będą mogły reagować na zdarzenia zarejestrowane przez czujniki np. wysłanie pomocy drogowej w sytuacji awarii pojazdu lub wysłanie hydraulika w przypadku wzrostu wilgotności podłogi w pomieszczeniach;
- łatwiejsza i prostsza stanie się likwidacja szkód – ubezpieczony nie będzie musiał zgłaszać szkody. Ubezpieczyciel poprzez analizę danych będzie mógł samodzielnie wydedukować na podstawie zmian otrzymywanych parametrów, że wystąpiło zdarzenie objęte ubezpieczeniem: stłuczka, zalanie, pożar;
- przeciwdziałanie przestępstwom na szkodę ubezpieczycieli – weryfikacja rzeczywistych danych z danymi otrzymanymi od klienta.

BEZGOTÓWKOWE, MOBILNE PARKOWANIE Z SYSTEMEM ROZPOZNAWANIA TABLIC REJESTRACYJNYCH

HTTPS://WWW.MONTERAIL.COM/BLOG/PARKING-SYSTEM-SOFTWARE-ADMYT
AUSTRIA / POLSKA

PROBLEM

Parkowanie samochodu na parkingach prywatnych, np. w centrach handlowych, związane jest z koniecznością uiszczenia opłaty w automatycznych kasach na podstawie informacji zapisanej na wcześniej pobranym przez użytkownika bilecie. To wiąże się z licznymi niedogodnościami, jak: zgubienie biletu, kolejki przy kasach czy brak gotówki.

ROZWIĄZANIE

Aplikacja mobilna admyt daje możliwość parkowania z pominięciem opisanych komplikacji. Wygodny proces rejestracji pozwala na połączenie konta z numerem rejestracyjnym samochodu, a umieszczone przy wjeździe na parking kamery, skanują nadjeżdżający pojazd i otwierają szlaban, rozpoczynając tym samym odliczanie czasu parkowania. Aplikacja na bieżąco informuje użytkownika o naliczonej należności. Przy wyjeździe z parkingu opłata zostaje pobrana z konta, a podsumowanie parkowania wraz z rachunkiem pojawia się w aplikacji. Aktualnie rozwiązanie wdrożono w 14 lokalizacjach typu centrum handlowe na terenie RPA. W planach – Pasaż Grunwaldzki, Wrocław (data uruchomienia 03/04.2019).

KORZYŚĆ

Zorientowany na użytkownika proces rejestracji, niezawodny i bezpieczny system płatności.

Zakres możliwego wykorzystania IoT

W najbliższych latach nastąpi więcej zmian w sposobie przeprowadzania transakcji przez ludzi niż w ciągu ostatnich kilku dekad. Technologia IoT wymagać będzie daleko idących zmian postaw klientów i partnerów wobec dzielenia się informacjami. Zmiana doświadczenia klienta łączy się z dbałością o bezpieczeństwo transakcji płatniczych (np. poprzez **biometrię**, czy **tokenizację**). Opomiarowanie produktów i przedmiotów codziennego użytku wpłynie w sposób bezpośredni i pośredni na świadczenie usług ubezpieczeniowych, płatniczych i finansowych.

Technologia IoT będzie szansą dla branży finansowej, ubezpieczeniowej i płatniczej na wprowadzenie zupełnie nowych produktów i usług opartych na informacjach otrzymywanych z czujników oraz ich późniejszej analizie. Nowoczesne rozwiązania płatnicze pozwolą na wprowadzenie nowych taryf i nowych metod zarządzania flotą pojazdów komunikacji miejskiej oraz obniżenie kosztów infrastruktury służącej do obsługi biletów w komunikacji miejskiej.

Ponad 20 miliardów **urządzeń połączonych** (ang. *connected devices*) do roku 2020 doprowadzi do gigantycznego wzrostu liczby miejsc, w których może odbywać się bezpieczny handel. Płatności stają się coraz bardziej „niewidoczne" (w tle), ułatwiając konsumentom korzystanie z usług online i **F2F** (np. Netflix, Uber). Tokenizacja urządzeń pozwoli na zwiększenie gamy narzędzi płatniczych i potencjalny wzrost transakcyjności.

TELEMATYKA W UBEZPIECZENIACH KOMUNIKACYJNYCH

HTTPS://PAYHOWYUDRIVE.PL/
POLSKA

PROBLEM

Obecnie wycena ubezpieczenia OC czy AC opiera się na statycznych elementach (np. wiek, rodzaj samochodu), nie uwzględniających zachowania kierowcy na drodze. Algorytm nie uwzględnia osób, które jeżdżą bezpiecznie, a mimo to znajdują się w grupie oznaczonej jako ryzykowna (np. młodzi ludzie). Dodatkowo, osoby jeżdżące niebezpiecznie mogą być sklasyfikowane w grupie mniejszego ryzyka. W związku z tym, kwota składki określana jest w nieadekwatny sposób.

ROZWIĄZANIE

YU! to oferta wypracowana przez Yanosik i ERGO Hestia bazująca na rozwiązaniu, które uzależnia cenę ubezpieczenia od stylu jazdy. YU! to pierwsza, powszechna oferta typu Pay-How-You-Drive („płacisz tak jak jeździsz").
YU! oferuje użytkownikom aplikacji Yanosik cenę ubezpieczenia bazującą na oszacowaniu ryzyka opartego o analizę stylu jazdy pod kątem bezpieczeństwa. Brana pod uwagę jest między innymi dynamika, sposób zachowania w niebezpiecznych punktach i przestrzeganie przepisów drogowych. Kierowca może budować swoją historię drogową poprzez jazdę z włączoną aplikacją Yanosik – urządzeniem rejestrującym parametry jazdy staje się telefon komórkowy (smartphone).

KORZYŚĆ

Celem ubezpieczenia YU! jest docenienie kierowców, którzy jeżdżą bezpiecznie. Właśnie do nich, za pośrednictwem aplikacji mobilnej Yanosik, może trafić oferta najtańszego ubezpieczenia OC, AC, Assistance i NNW. Bezpieczni kierowcy otrzymają zindywidualizowaną ofertę.

Rząd RP oraz podległe mu instytucje publiczne (m.in. Krajowa Administracja Skarbowa, Ministerstwo Finansów, Ministerstwo Przedsiębiorczości i Technologii, Główny Urząd Miar) planują wymianę blisko 2 milionów kas fiskalnymi, które potencjalnie mogą stać się urządzeniami klasy IoT. Zastosowanie IoT może wesprzeć implementację koncepcji tzw. fiskalizacji online.

Sektor finansowo-ubezpieczeniowy planuje wykorzystać technologię IoT w zakresie:

- automatyzacji i usprawniania dotychczasowych procesów i usług,
- budowy i oferowania klientom zupełnie nowych kategorii produktów i usług,
- minimalizacji i optymalizacji ryzyk realizowanych procesów (np. monitoring stanów i parametrów przedmiotów objętych ubezpieczeniem oraz identyfikowania ryzyk i reagowania na nie w celu ograniczenia konsekwencji ich wystąpienia),
- zwiększenia integracji usług i rozliczeń w relacjach B2B i B2C,
- automatyzacja procesów likwidacji szkód i wypłat roszczeń w ubezpieczeniach,
- zwiększenie integracji usług i rozliczeń w relacjach B2B i B2C,

- integracji usług opartych o IoT (zmiany stanów z czujników) z usługami mikropłatności i podatkowymi.

Bariery

W toku prac podgrupa zidentyfikowała następujące bariery dla branży:

- Brak wystarczających kompetencji i możliwości wykorzystania potencjału technologii IoT w sektorze.

- Niechęć i obawy klientów i partnerów biznesowych do udostępniania danych informujących o sposobie używania przez nich przedmiotów i produktów codziennego użytku, gdzie duży potencjał widzi branża ubezpieczeniowa.

- Brak klarownych, precyzyjnych regulacji w zakresie sposobu klasyfikowania poszczególnych strumieni danych IoT, sposobu ich ochrony oraz zasad przesyłania i przetwarzania.

- Ograniczenia prawne w zakresie klasyfikowania danych pochodzących z czujników IoT, wymiany tych danych, ich przechowywania i przetwarzania. Sektor finansowy jako sektor regulowany szeregiem restrykcyjnych przepisów będzie miał trudność w efektywnym wykorzystaniu tej technologii. Niezbędne wydają się zmiany w przepisach dotyczących tajemnic branżowych oraz RODO.

Propozycje działań rządu

Zmiany technologiczne muszą korespondować ze zmianami prawa i regulacjami nadzorczymi, by wykorzystać potencjał drzemiący w technologii IoT, w szczególności w sektorze tak wysoce regulowanym i nadzorowanym jakim jest sektor finansowo-ubezpieczeniowy. W związku z tym, rekomendujemy następujące działania:

- Wsparcie samorządów we wdrażaniu i standaryzacji nowych metod płatności za transport publiczny poprzez instalację czujników typu bluetooth beacon w pojazdach komunikacji miejskiej oraz na przystankach.

- Wdrożenie spójnych ram legislacyjnych – innowacyjność wdrażanych rozwiązań powinna współgrać z otwartością podmiotów publicznych na przyjmowanie zmian (dostosowanie legislacji, otwarte formuły przetargowe, uwzględnianie czynnika innowacyjności w stosowanych kryteriach).

- Opracowanie klarownych przepisów, pozwalających na jednoznaczną klasyfikację danych IoT, ich ochronę, przetwarzanie oraz transfer.

- Dostosowanie przepisów ustawy o działalności ubezpieczeniowej i RODO do możliwości przetwarzania danych IoT. W szczególności wymagane jest wypracowanie rozwiązań pozwalających na wyłączenia danych IoT z tajemnic sektorowych oraz sposobu ich traktowania w kontekście przepisów RODO.

- Uregulowanie kwestii ubezpieczeń komunikacyjnych opartych o zachowanie kierowców (indywidualne stawki oparte o ocenę stylu jazdy).

- Dokonanie redefinicji protokołów wymiany danych z Internetem dla kas fiskalnych online i zmiany standardów zapisów paragonów, w celu redukcji kosztu urządzeń i przyśpieszenia wdrożenia fiskalizacji online oraz nowych metod płatniczych, przy jednoczesnym zmniejszeniu nakładów inwestycyjnych Rządu RP (z 320 mln zł) i przedsiębiorców (z 3 mld zł) w ciągu kolejnych 10 lat. Postulujemy wyniesienie pamięci fiskalnej z urządzenia do warstwy aplikacyjnej (np. w chmurze i z opcjonalnym zabezpieczeniem kryptograficznym opartym o blockchain) celem przyspieszenia i obniżenia kosztu fiskalizacji online oraz wsparcia adopcji nowych metod płatniczych i e-paragonu.

10

INTELIGENTNE MIASTA I BUDYNKI

Dzięki technologii Internetu Rzeczy i rozwojowi technologii ICT nasze miasta mają szansę stać się bardziej przyjazne mieszkańcom, lepiej zorganizowane i efektywniej wykorzystujące dostępne zasoby. W długim horyzoncie czasowym, realizacja koncepcji Inteligentnych Miast, może zaś stanowić istotną siłę napędową polskiej gospodarki, przynosząc wymierne korzyści dla mieszkańców, jednostek administracji publicznej, oraz przedsiębiorstw prywatnych.

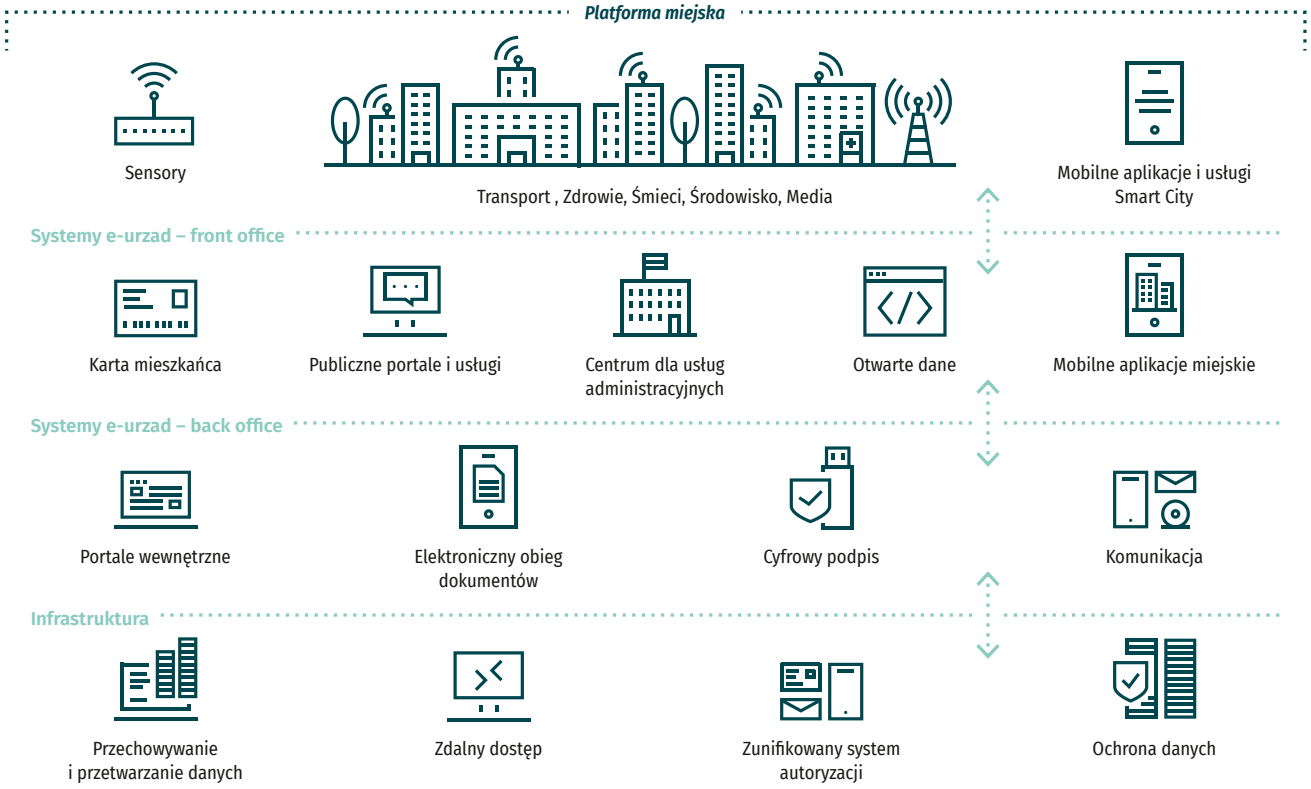
AUTORZY:
REMIGIUSZ WIŚNIEWSKI, DETECON INTERNATIONAL GMBH – LIDER PODGRUPY
MICHAŁ BAŁOS, EMITEL S.A.
KRYSTIAN BERGMANN, FIBAR GROUP S.A.
DAMIAN KLIMAS, UNIWERSYTET WROCŁAWSKI
FRANCISZEK MAROSZEK, NOKIA SOLUTIONS AND NETWORKS S P. Z O.O. I STOWARZYSZENIE HACKERS PACE WROCŁAW
MIROSŁAW POLSKI, HEWLETT PACKARD ENTER PRISE POLSKA S P. Z O.O.
MATEUSZ STEFAŃSKI, MICROSOFT
ARNOLD WIERZEJSKI, NOKIA

Ogólna charakterystyka branży

Mianem Inteligentnego Miasta (ang. *Smart City*) określa się przestrzeń, która „wykorzystuje technologie informacyjno-komunikacyjne w celu zwiększenia interaktywności i wydajności infrastruktury miejskiej i jej komponentów składowych, a także do podniesienia świadomości mieszkańców." Miasto może być traktowane jako „inteligentne", gdy podejmuje inwestycje w kapitał ludzki i społeczny oraz infrastrukturę komunikacyjną, w celu aktywnego promowania zrównoważonego rozwoju gospodarczego i wysokiej jakości życia, w tym mądrego gospodarowania zasobami naturalnymi, przez partycypację obywatelską[1], co powinno przekładać się m.in. na:

- powszechny dostęp do informacji o mieście jak i o planach jego rozwoju itp.,
- sprawną, efektywną oraz pro-ekologiczną komunikację,
- optymalne wykorzystanie infrastruktury miejskiej i zasobów z których mieszkańcy korzystają (energia elektryczna, gaz, ciepło),
- dbałość o stan środowiska, w szczególności przekładająca się na niski poziom zanieczyszczeń,
- bezpieczeństwo mieszkańców,
- poprawę jakości, efektywności i dostępności usług związanych z ochroną zdrowia,
- sprawne załatwianie spraw w urzędach i instytucjach miejskich,
- korzystne warunki do inwestowania w mieście,
- efektywne działanie służb miejskich,
- wiele możliwości spędzania wolnego czasu (wydarzenia kulturalne, imprezy sportowe itp.),
- aktywny udział mieszkańców w ulepszaniu miasta poprzez współpracę z administracją,
- zapewnienie równych szans i warunków różnym grupom społecznym.

Osią koncepcji Inteligentnych Miast jest cyfryzacja przestrzeni miejskiej, której celem jest tworzenie miast, które byłyby bardziej przyjazne dla mieszkańca, bardziej ekonomiczne i ekologiczne. Z technologicznego punktu widzenia, kluczowym elementem umożliwiającym wdrożenie tej idei jest Internet Rzeczy, czyli zgodnie z przedstawioną definicją w rozdziale 3, koncepcja bazująca na łączności między urządzeniami (M2M – machine to machine) zakładająca możliwość komunikacji, gromadzenia i przetwarzania danych oraz ich wymiany przez te urządzenia za pomocą sieci komputerowej. W dużym uproszczeniu oznacza to oczujnikowanie przestrzeni miejskiej, domów i budynków, aby umożliwić monitorowanie zdarzeń w czasie rzeczywistym i/lub wymianę informacji między zarówno maszynami, jak i ludźmi. Zwiększenie poziomu dostępu do informacji np. o ruchu ulicznym, poziomie zajętości miejsc parkingowych czy też potrzebnemu natężeniu światła pozwoli istotnie zoptymalizować wykorzystanie dostępnych zasobów, a także usunąć wiele wąskich gardeł w infrastrukturze miejskiej. Zarys koncepcji obrazuje poniższy rysunek:



1 Azkuna I. (red.), Smart Cities Study: International study on the situation of ICT, Innovation and Knowledge in Cities. Bilbao, 2012

Mając powyższe na uwadze, realizacja koncepcji Inteligentnego Miasta obejmuje swoim zasięgiem właściwie większość obszarów urbanistycznych, w szczególności:

- Transport & Mobilność (np. rozwiązania optymalizujące ruch miejski (Inteligentny Transport), współdzielenie pojazdów (*Car/Bike Sharing*), inteligentne parkingi i przystanki)
- Zarządzanie odpadami (np. monitorowanie odpadów w czasie rzeczywistym, śledzenie odpadów nieprzetworzonych)
- Środowisko (badanie poziomu zanieczyszczenia środowiska / powietrza w czasie rzeczywistym, monitoring rzek i zbiorników wodnych)
- Oświetlenie dróg i infrastruktury miejskiej (inteligentne lampy tj. sterowanie oświetleniem i monitorowanie pracy latarni oraz otoczenia)
- Domy i budynki (inteligentne budynki i automatyka budynkowa)
- Bezpieczeństwo (np. monitorowanie przestrzeni publicznej, identyfikacja przestępstw, systemy reagowania w sytuacjach kryzysowych, zarządzanie zgromadzeniami i tłumem)
- Dostarczanie mediów (np. monitorowanie zużycia, wykrywanie anomalii etc.)
- Zdrowie (np. urządzenia medyczne do pomiaru parametrów fizjologicznych, zdalne monitorowanie pacjenta, zdalne prowadzeni terapii).

Większość przedstawionych powyżej obszarów zastosowań znajduje się w zakresie odpowiedzialności gmin, więc naturalnym wydaje się, że głównym sponsorem takich wdrożeń będą jednostki samorządowe. Samorządy, obok dostawców rozwiązań, mają bowiem największe motywacje do tworzenia miast inteligentnych:

- tańsza realizacja zadań własnych gminy,
- poprawa jakości środowiska (np. jakości powietrza),
- poprawa jakości życia dla mieszkańców,
- zwiększenie dostępności usług i informacji dla mieszkańców,
- zwiększenie zatrudnienia,
- dodatkowy kapitał polityczny.

Identyfikacja barier oraz przygotowanie rekomendacji dla branży Inteligentnych Miast i budynków powinny więc w istotnym zakresie obejmować jednostki samorządowe.

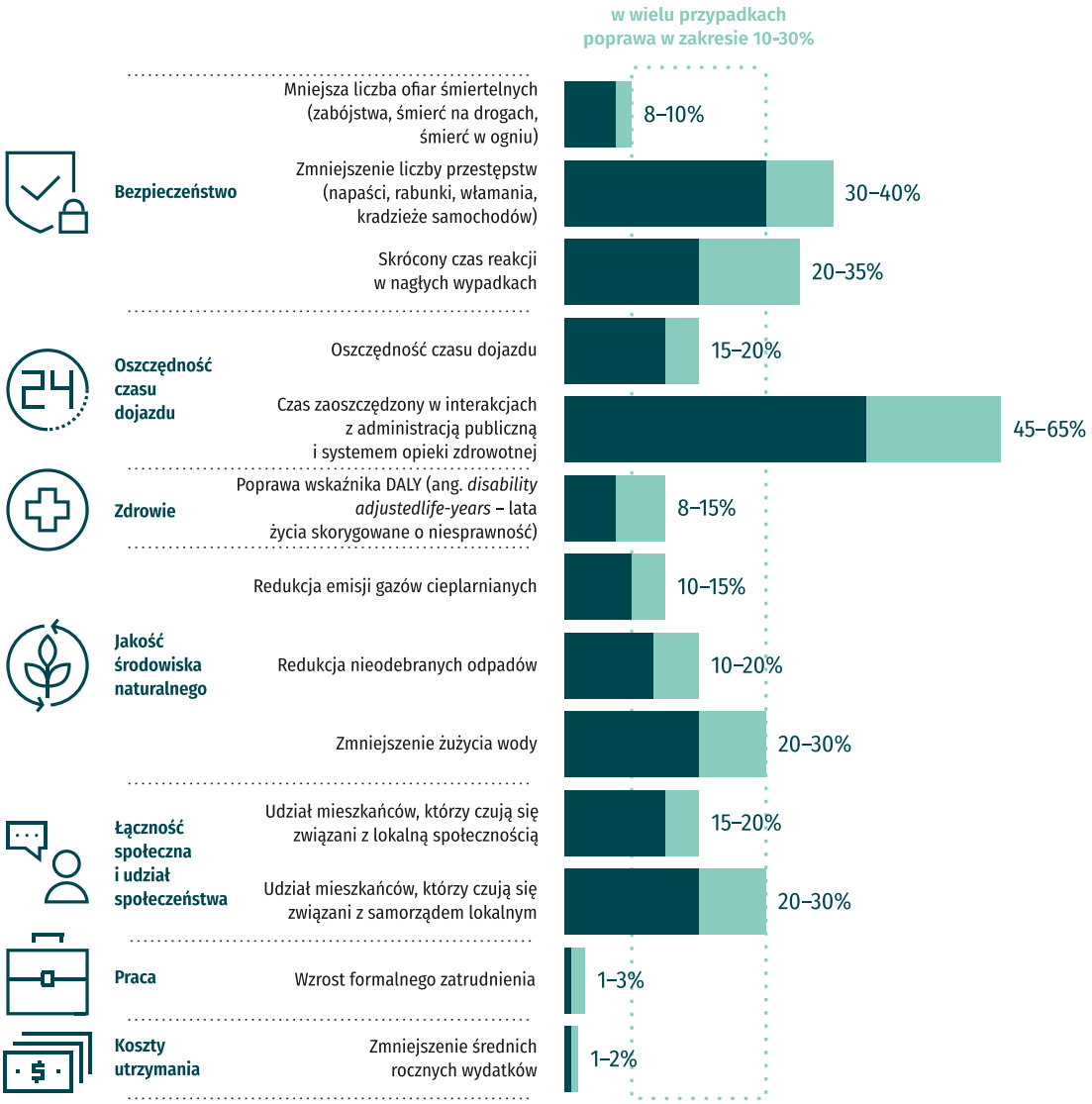
Przedstawione powyżej przykłady zastosowań obrazują branżę Inteligentnych Miast i Budynków z perspektywy popytowej, gdzie bezpośrednim beneficjentem są samorządy, przedsiębiorstwa użyteczności publicznej oraz mieszkańcy. Mając jednak na uwadze cele niniejszego raportu należy również wziąć pod uwagę perspektywę podażową tj. rynek dostawców rozwiązań w całym łańcuchu wartości związanym ze Smart City, są to m.in.:

- sensory, kamery i inne urządzenia gromadzące i wysyłające dane,
- urządzenia zapewniające łączność realizowaną za pośrednictwem różnych protokołów zarówno w paśmie licencjonowanym jak i nielicencjonowanym (GPRS, 3G, 4G, LoRaWAN, LoRa, Sigfox, 868 MHz, 900 MHz, NB IoT, LTE Cat0, LTE Cat1, LTE Cat M ZigBee, 802.15.4, Wi-Fi, RFID, NFC, Bluetooth 4.0, Z-Wave i HomeKit),
- platformy mediacyjne, szyny integracyjne,
- systemy do zarządzania danymi,
- zasoby obliczeniowe (*cloud computing*),
- systemy raportowe i analityczne, AI,
- systemy bezpieczeństwa,
- warstwa aplikacyjna dostarczająca usługi końcowe.

W każdym z wyżej wymienionych segmentów można oczekiwać znacznego potencjału rozwojowego przy czym nie w każdym obszarze ten potencjał będzie jednakowy, m.in. ze względu na obecną liczbę graczy i różne bariery wejścia. Mając jednak na uwadze potencjał rozwojowy rynku lokalnego, europejskiego i globalnego, perspektywy rozwojowe dla rodzimych dostawców wydają się być bardzo duże. Wymaga to jednak działań wielokierunkowych stymulujących zarówno popyt tj. istotnie zwiększających poziom inwestycji w zakresie Smart City w Polsce, jak i działań wspierających firmy działające na tym rynku.

Perspektywa rozwoju branży

Rynek rozwiązań związanych z ideą Smart City dynamicznie się rozwija, adresując wiele wyzwań związanych z gwałtowną urbanizacją, przy czym należy w tym miejscu mieć na względzie, iż procesy te będą się jeszcze pogłębiać. Prognozy wskazują iż do roku 2050 w miastach ma mieszkać ponad 80 proc. populacji krajów rozwiniętych i ponad 60 proc. mieszkańców krajów rozwijających się. Można więc oczekiwać, że dzisiejsze problemy związane z zanieczyszczeniem środowiska, dostępnością infrastruktury, komunikacją publiczną i transportem prywatnym, odpadami, rosnącym zapotrzebowaniem energetycznym będą się jedynie nasilać. W konsekwencji włodzarze miast będą zmuszeni do podjęcia pilnych działań zaradczych, a realizacja koncepcji Inteligentnych Miast i Budynków może okazać się pomocna przy rozwiązywaniu przynajmniej części z problemów. Oczekiwane korzyści przedstawia wykres na stronie 35.



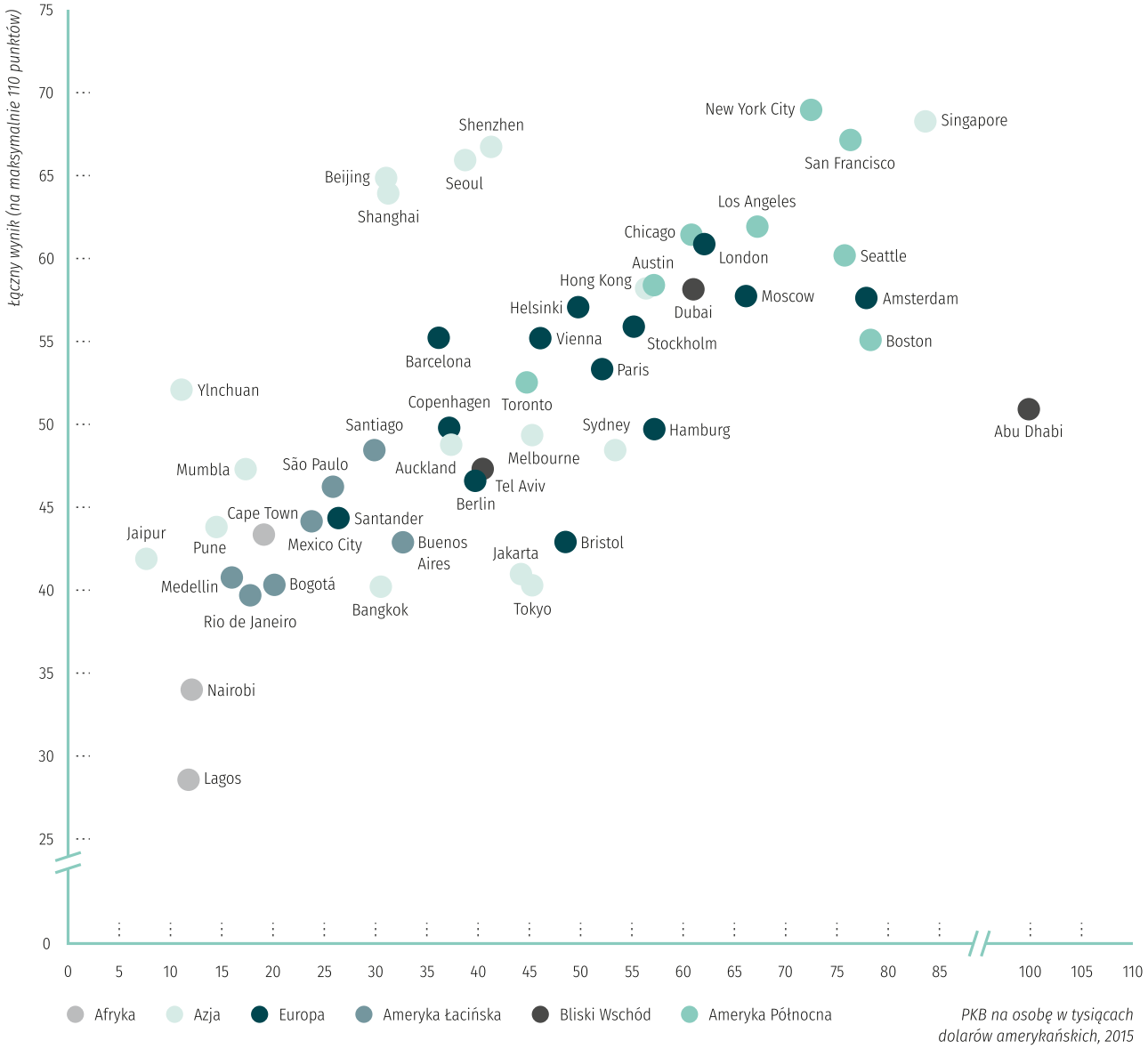
Według badania przeprowadzonego przez IAB Polska w 2015 roku korzyści płynące z wykorzystania IoT wg polskich internautów są następujące:

Źródło: IAB Polska, „Internet Rzeczy": maj 2015, internauci w wieku 15+, N=1221, realizacja: Webankieta.pl.

Wyzwania związane z urbanizacją to oczywiście nie jedyny element wpływający na rozwój Inteligentnych Miast, z istotnych czynników należy wymienić:

- rozwój ekonomiczny,
- polityka zrównoważonego rozwoju,
- konieczność podjęcia zdecydowanych działań na rzecz ochrony środowiska globalnie,
- bezpieczeństwo publiczne,
- zwiększenie liczby samochodów – szacowany 1 miliard samochodów do 2020 r.,
- dostępność infrastruktury telekomunikacyjnej,
- rozwój i poprawa dostępności technologii (sztuczna inteligencja, Internet Rzeczy, 5G, blockchain),
- dostęp do Big Data i możliwości analizy i podejmowania decyzji na ich podstawie (dane z systemów, aplikacji, czujników IoT),
- digitalizacja w różnych dziedzinach i obszarach gospodarki,
- oczekiwania społeczne i wymogi nowych generacji.

Dlatego też wiele krajów i miast podejmuje wysiłki w celu wdrożenia w szerszym zakresie idei Inteligentnego Miasta. Poniższy wykres prezentuje zestawienie miast wdrażających Smart City.



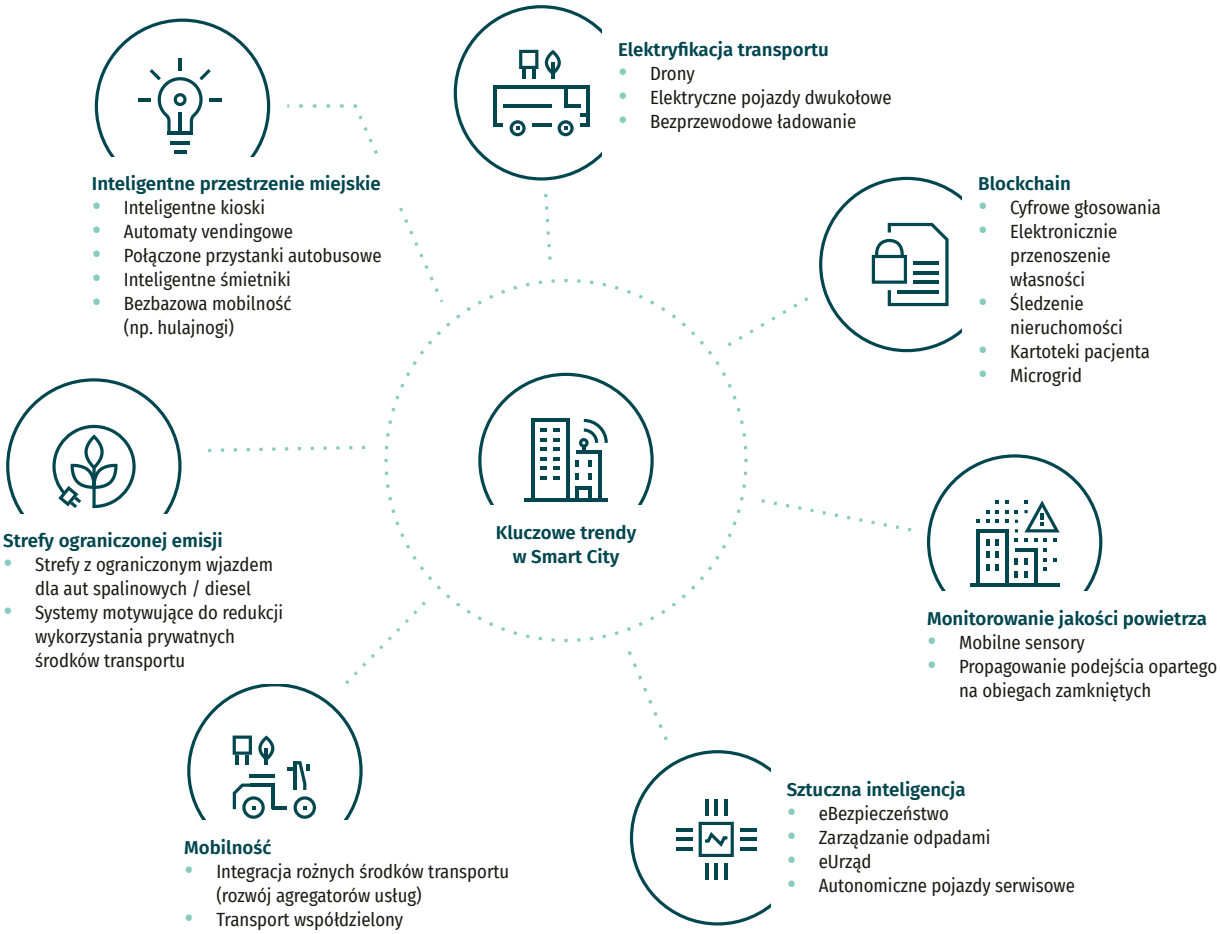
Źródło: McKinsey Global Institute CityScope database

Przekłada się to na prognozy rozwoju całej branży. Instytut Machina Research oraz McKinsey szacują wielkość globalnego rynku IoT dla zastosowań Smart City na aż 10 bilionów EUR do końca 2025[1] roku. Frost & Sullivan jest nieco ostrożniejszy w szacunkach, wskazując na potencjał rzędu 2 bilionów dolarów w podobnym horyzoncie czasowym, natomiast w każdym z tych przypadków potencjał ten jest bardzo duży. Podobnie sytuacja przedstawia się w poszczególnych segmentach np. według analiz branżowych inteligentne budynki posiadają największy potencjał rozwojowy konsumenckiej gałęzi Internetu Rzeczy. Branża inteligentnego domu rośnie z dynamiką 38% rocznie w Europie i do 2020 roku może być warta nawet 20 miliardów dolarów. Szacuje się także, że liczba gospodarstw domowych wyposażonych w automatykę w Unii Europejskiej wzrośnie z 13 milionów w 2018 r. do 27 milionów w 2020. Największy potencjał nabywczy posiadają urządzenia związane z oszczędnością zużycia energii i bezpieczeństwem bliskich.

Grupa Robocza nie dysponowała danymi na podstawie których można byłoby oszacować potencjał w Polsce. Można jednak oczekiwać, że zarówno dynamika wzrostu jak i potencjał w dłuższym horyzoncie czasowym będą korespondować z trendami globalnymi a umiejętne ich wykorzystanie może stanowić istotny motor rozwojowy polskiej gospodarki. Szczególnie, że obecnie rozwiązania w omawianym zakresie są wdrażane bardzo selektywnie i silosowo, głównie koncentrując się na inteligentnym oświetleniu, ITS (Inteligentnych Systemach Transportowych) i jakość życia w polskich miastach jest relatywnie niska w porównaniu z liderami światowych rankingów. Rozwojowe segmenty w najbliższej perspektywie czasowej na rynku polskim to:

- segmenty będące w kręgu zainteresowań UE dla Smart City (budżet UE, zatem wymagania UE),
- infrastruktura i środowisko: ochrona środowiska, woda i energia, transport,
- podstawowe usługi publiczne: bezpieczeństwo publiczne, służba zdrowia, edukacja,
- planowanie i zarządzanie: inteligentne budynki, *open government*, inteligencja zarządzania i planowania,
- łatwiejszy dostęp do danych i urzędów,
- poprawa bezpieczeństwa i podniesienie wygody,
- poprawa warunków środowiskowych.

Planowanie długoterminowe powinno uwzględniać też trendy światowe wskazujące na rosnącą adopcję rozwiązań z zakresu elektromobilności, wykorzystanie aut autonomicznych, czy też wykorzystania blockchain w różnych, przedstawionych na poniższym diagramie, obszarach.



Działania katalizujące realizację koncepcji Inteligentnych Miast i Budynków na szeroką skalę – ze strony popytowej i podażowej – mogą przynieść wiele korzyści w wymiarze społecznym i finansowym dla miast, mieszkańców, przedsiębiorstw pożytku publicznego oraz firm prywatnych tworzących rozwiązania. Może to stymulować wzrost społeczno-gospodarczy, przyczyniając się do zwiększenia konkurencyjności polskiej gospodarki. Z drugiej strony, mając na uwadze obecne trendy i dużą dynamikę zmian w globalnej gospodarce, można zaryzykować twierdzenie, iż zaniedbanie obecnej szansy, którą daje rewolucja technologiczna związana z IoT, Przemysłem 4.0, sztuczną inteligencją, 5G może spowodować w dłuższym horyzoncie czasowym istotne obniżenie wydajności i konkurencyjności polskiej gospodarki na tle innych krajów rozwiniętych.

Zakres możliwego wykorzystania IoT

Urządzenia IoT są jednym z technologicznych fundamentów Miast Inteligentnych, to dzięki nim możliwe jest zdalne nadzorowanie i sterowanie infrastrukturą miejską. Zakres możliwego wykorzystania tej technologii jest bardzo szeroki, gdyż realizacja koncepcji Inteligentnych Miast polega de facto na integracji wielu obszarów i wykorzystaniu potencjału gromadzonych danych w różnych kontekstach. W połączeniu z pozostałą infrastrukturą IT urządzenia stanowiące Internet Rzeczy tworzą inteligentne systemy, wśród których najczęściej spotykane zastosowania z perspektywy Miast Inteligentnych to:

- zarządzanie mediami (oświetlenie miejskie, dostawy wody/prądu, wywóz odpadów),
- monitoring przestrzeni publicznej,
- monitoring zanieczyszczeń środowiska,
- systemy transportowe (ITS – Inteligentne Systemy Transportowe, Inteligentne Parkingi),
- współdzielenie pojazdów,
- ochrona zdrowia mieszkańców.

Zakres wykorzystania IoT w ramach realizacji koncepcji Inteligentnych Miast i Budynków

Rozwiązanie	Opis	Korzyści
Inteligentny Transport (ang. *Smart Transport*)	Szeroka grupa rozwiązań zwiększających zarówno poziom informowania jak i wymiany informacji między uczestnikami miejskiej sieci transportowej, których celem jest zapewnienie bezpieczniejszej i efektywniejszej infrastruktury komunikacyjnej. Rozwiązania te potrafią identyfikować i reagować na zmienne warunki na drogach, wytyczając optymalne dla kierowców trasy, a także optymalizować zużycie paliwa. W szczególności są to Inteligentne Systemy Transportowe (ang. *ITS*) zbierające informacje zarówno z dostępnych źródeł – czujników, kamer, urządzeń zamontowanych w pojazdach transportu zbiorowego, stacji meteorologicznych, fotoradarów itp. Stała komunikacja pomiędzy poszczególnymi urządzeniami w połączeniu z systemami zaawansowanej analizy danych ma w założeniu pozwolić firmom transportowym przewidzieć awarie lub usterki, dzięki czemu uniknęłyby one w przyszłości kosztownych napraw i związanych z nimi przestojów.	• Zwiększenie przepustowości infrastruktury transportowej. • Poprawa bezpieczeństwa. • Skrócenie czasu podróży, ograniczenie zużycia paliwa i energii. • Poprawa efektywności transportu publicznego (redukcja kosztów taboru). • Efektywne zarządzanie kryzysowe.
Współdzielenie rowerów/ samochodów (ang. *Bike/Car Sharing*)	Systemy współdzielenia pojazdów za pomocą aplikacji mobilnej umożliwiają wypożyczenie na krótki okres roweru/ samochodu/ skutera/ hulajnogi elektrycznej na obszarze miasta. Rozwiązania tego typu rozwiązują m.in. problemy dojazdu w obszary słabo skomunikowane czy też problem „ostatniej mili" (dotarcie z przystanku do oddalonego od niego celu). Dostępność systemów współdzielenia samochodów może też prowadzić do obniżenia potrzeby posiadania samochodu wśród mieszkańców.	• Mniejsza ilość samochodów wjeżdżających do miast/ lepsze wykorzystanie przestrzeni w centrach miast. • Większa elastyczność transportu publicznego. • Większa utylizacja pojazdów.

Rozwiązanie	Opis	Korzyści
Inteligentne Parkingi (ang. *Smart Parking*) – czujniki zajętości miejsc parkingowych	Celem Inteligentnych Parkingów jest przede wszystkim optymalizacja wykorzystania miejsc parkingowych. Biorąc pod uwagę, że kilkadziesiąt procent ruchu w centrach miast generują kierowcy szukający miejsc do parkowania, ułatwienie znalezienia wolnego miejsca znacząco ogranicza ruch samochodowy w okolicy. Za pomocą sensorów zainstalowanych w pobliżu miejsc parkingowych pozyskiwane są informacje o lokalizacji wolnego miejsca, liczbie przejeżdżających pojazdów, czy nawet ich prędkości i wielkości. Informacje o wolnych miejscach są następnie przekazywane kierowcom.	• Optymalne wykorzystanie miejsc parkingowych, wyższe wpływy z opłat. • Ułatwione znajdowanie wolnych miejsc parkingowych.
Monitoring zanieczyszczeń powietrza (ang. *Air Quality Monitoring*) – czujniki zanieczyszczeń powietrza	Umieszczenie w newralgicznych punktach przestrzeni miejskiej czujników mierzących jakość powietrza pomaga diagnozować jego skład pod kątem zawartości szkodliwych gazów (np. tlenków siarki/azotu/węgla) czy pyłów zawieszonych (PM10 i PM2,5). Informacje tego typu ułatwiają lokalizowanie źródeł zanieczyszczeń oraz umożliwiają wczesne ostrzeganie o przekroczeniach norm, co ma istotny wpływ na zdrowie mieszkańców miasta.	• Lepszy nadzór nad jakością powietrza. • Łatwiejsze lokalizowanie źródeł zanieczyszczeń. • Szybsze informowanie mieszkańców o przekroczeniach norm.
Inteligentne oświetlenie (ang. *Smart Lighting*)	Inteligentne oświetlenie miejskie, wykorzystujące czujniki natężenia ruchu pieszego i samochodowego w najbliższym otoczeniu, spełnia dwie funkcje – doświetla skrzyżowania w celu poprawy bezpieczeństwa oraz oszczędza energię obniżając jasność w sytuacjach braku ruchu w okolicy.	• Obniżone zużycie energii, niższe koszty oświetlenia miejskiego. • Zwiększone bezpieczeństwo w ruchu drogowym.
Inteligentny budynek (ang. *Smart Home*)	Inteligentny budynek to system czujników i urządzeń wykonawczych posiadający jeden, zintegrowany system zarządzania, pozwalający na zdalny dostęp do danych. Dzięki danym płynącym z czujników system może automatycznie reagować na zmiany poprzez interakcję z użytkownikiem lub własny, zaprogramowany zestaw instrukcji. Elementarne funkcje automatyki budynkowej można podzielić na poniższe obszary (w kontekście sterowania, monitoringu, optymalizacji i raportowania): • Sterowanie oświetleniem i dowolnymi odbiornikami energii elektrycznej • Sterowanie roletami, bramami, systemami kontroli dostępu • Sterowanie klimatem wewnątrz budynków (kontrola temperatury, jakość powietrza, wentylacja) • Ochrona zdrowia, życia i mienia (detektory, przetworniki, monitoring wizyjny, systemy alarmowe) • Integracja z urządzeniami elektroniki powszechnego użytku (RTV i AGD) • Monitoring i optymalizację produkcji i zużycia energii • Obszary zastosowań inteligentnych budynków dotyczą zarówno obiektów użyteczności publicznej, komercyjnych jak i budownictwa mieszkaniowego.	• Zmniejszenie zużycia mediów (prąd, gaz, woda) • Poprawa bezpieczeństwa mieszkańców. • Poprawa komfortu życia mieszkańców.

Rozwiązanie	Opis	Korzyści
Inteligentne Bezpieczeństwo (ang. *Smart Security*)	Grupa rozwiązań w różnych aspektach adresująca ochronę życia, zdrowia i mienia mieszkańców. Są to m.in.: • Inteligentne monitorowanie przestrzeni publicznej – systemy kamer i monitorowania otoczenia, (sensory ruchu, pożaru, zalania, obecności niebezpiecznych związków w powietrzu etc.). • Wykrywanie strzałów – rozwiązania obejmujące zarówno czujniki / kamery jaki i systemy wykrywające zdarzenia potencjalnie związane z przestępstwami bądź wypadkami. • Inteligentne systemy reagowania w sytuacjach kryzysowych. • Zarządzanie tłumem / zgromadzeniami – analityka tłumu – systemy monitorowania przemieszczania się mieszkańców oparte o dane telekomunikacyjne. • Inteligentne centra zarządzania kryzysowego, które agregują dane sensoryczne i analitykę video.	• Poprawa bezpieczeństwa fizycznego mieszkańców. • Ograniczenie przestępstw i wypadków oraz redukcja ewentualnych skutków. • Wykorzystanie infrastruktury i zasobów służb mundurowych.
Inteligentne opomiarowanie	Grupa rozwiązań pozwalających na automatyczny odczyt liczników mediów: • Detekcja wycieków. • Monitorowanie zużycia. • Monitorowanie jakości. • Inteligentny pomiar irygacji zbiorników i rzek. • Opomiarowanie gazu. Obszar inteligentnego opomiarowania został szerzej opisany w rozdziale 12.	• Ograniczenie zużycia mediów. • Redukcja awarii.
Inteligentna Ochrona Zdrowia	Szeroka grupa rozwiązań wykorzystujących IoT w połączeniu z systemami zaawansowanie analizy danych i sztucznej inteligencji do zdalnego diagnozowania i prowadzenia terapii. Obszar Ochrony Zdrowia został szerzej opisany w rozdziale 11.	• Obniżenie kosztów leczenia. • Poprawa jakości usług medycznych.

Przedstawiona powyżej lista nie jest oczywiście wyczerpująca, liczba zastosowań jest bowiem właściwie nieograniczona. Dzisiejsze możliwości technologiczne pozwalają bowiem na ulokowanie czujników w większości obiektów współczesnych miast oraz na gromadzenie i przetwarzanie ogromnych wolumenów danych, wysnuwanie wniosków, prognozowanie i przewidywanie zdarzeń. Dotychczasowe wyniki wdrożeń rozwiązań z zakresu Inteligentnych Miast wskazują na znaczące korzyści społeczne i finansowe, wynikające z tej technologii. Nowe systemy pozwalają m.in. na:

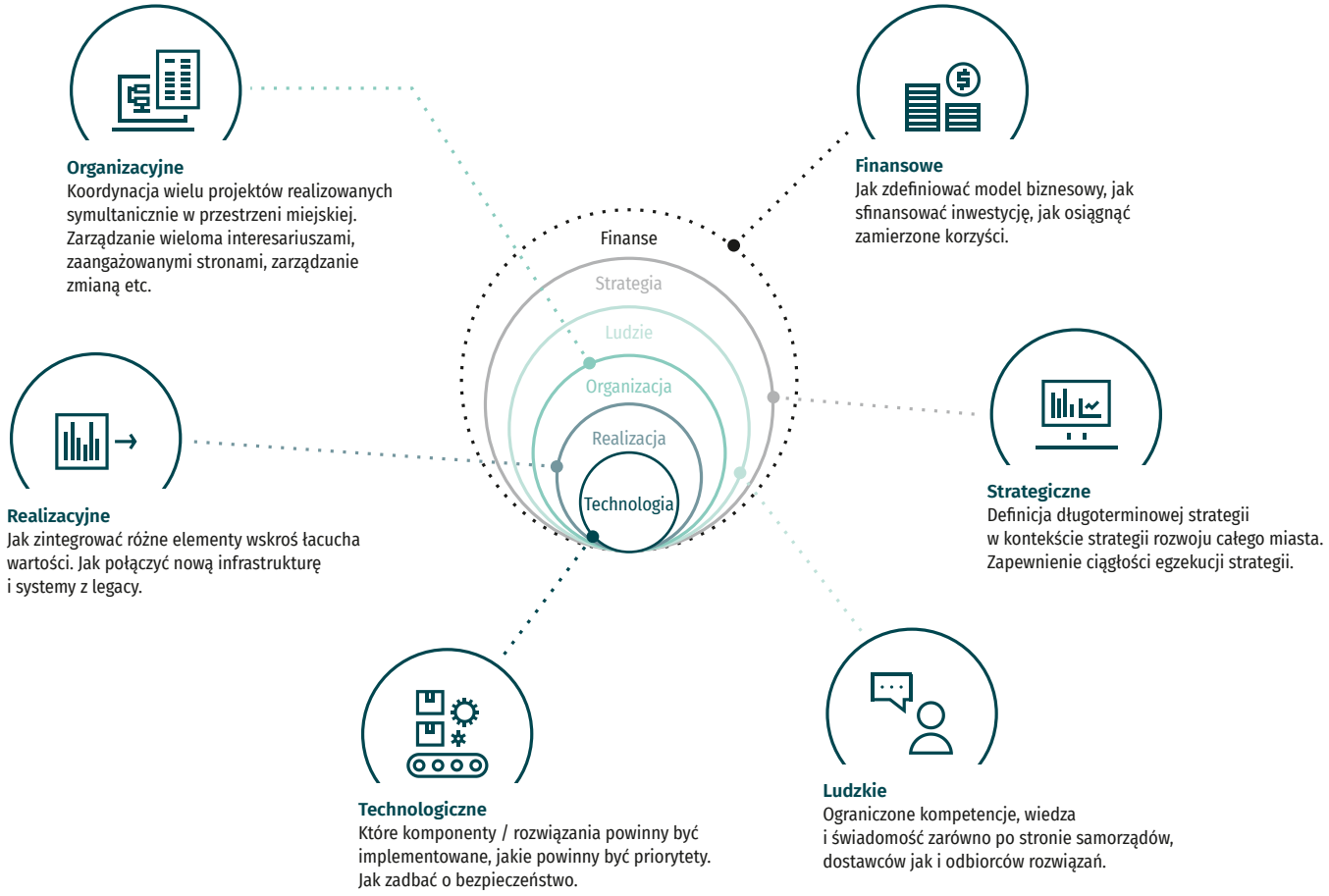
- zmniejszenie czasu podróży komunikacją miejską o 20%,
- zmniejszenie czasu poświęconego w urzędach o 65%,
- zmniejszenie czasu odpowiedzi na nagłe wypadki o 35%,
- zmniejszenie przestępczości o 40%,
- zmniejszenie kosztów życia i utrzymania mieszkańców o 3%,
- wzrost zatrudnienia o 3%,
- zmniejszenie szkodliwych emisji oraz zużycia wody o 15%.

Największe korzyści można uzyskać integrując poszczególne obszary, stąd konieczne jest spojrzenie holistyczne na całe zagadnienie. Warto również spojrzeć na podejście i przykłady wdrożeń rozwiązań w całych aglomeracjach miejskich.

Bariery

Rozwój technologii informacyjno-komunikacyjnych niewątpliwie przyczynia się do rozwoju w miastach koncepcji Smart City, ale jej wdrażanie często odbywa się w sposób niekontrolowany, wyspowy i niezintegrowany z innymi działaniami realizowanymi przez różne podmioty działające na terenie lokalnym. Skutkuje to powielaniem rozwiązań i stosowaniem różnych, niewspółpracujących standardów, co powoduje nieefektywność kosztową. Nawet na wspólnym terenie, jakim jest lokalna jednostka administracyjna, różne podmioty (administracja państwowa, podmioty publiczne oraz prywatne) działając w ramach swoich uprawnień oraz celów biznesowych mogą i najczęściej realizują swoje projekty w sposób nieskoordynowany, co uniemożliwia stworzenie zintegrowanej publicznej infrastruktury Smart City. Powielanie (np. infrastruktury) uniemożliwia korzystanie ze środków unijnych i ogranicza rozwój Smart City. Dotyczy to w szczególności Polski, gdzie dodatkowo poziom adopcji rozwiązań IoT w miastach jest bardzo niewielki.

Wynika to w szczególności z wielu wyzwań związanych z wdrażaniem rozwiązań z zakresu Smart City, przedstawionych na poniższym diagramie.



Równie istotnym problemem na obecnym etapie wdrażania rozwiązań z obszaru IoT jest ograniczone zainteresowanie potencjalnych klientów. Brakuje świadomości zarówno po stronie mieszkańców, jak i samorządów. Rozwój branży jest stymulowany przez dostawców, a nie przez realne potrzeby użytkowników. W wielu przypadkach potencjalne zalety tracą na znaczeniu w zderzeniu rzeczywistością. Ograniczenie organizacyjne, ekonomiczne i formalne powoduje, że potencjalni odbiorcy nie widzą potrzeby wdrażania tych rozwiązań, dlatego też bardzo istotnym elementem jest ocena rzeczywistych potrzeb. IoT nie może być postrzegane jedynie przez pryzmat nowości i źródła potencjalnych dodatkowych przychodów, powinno szczególnie w obszarze SmartCity odpowiadać na potrzeby mieszkańców i służyć poprawie życia w mieście.

Bariery znajdują się w różnych obszarach i na różnym etapie adopcji rozwiązań IoT w miastach. Poniżej przedstawione zostały główne bariery zidentyfikowane w trakcie prac Grupy Roboczej. Należy w tym miejscu zaznaczyć, że Inteligentne Miasta to ekosystem systemów, więc w ramach prac grupy niemożliwe było odniesienie się na niskim poziomie szczegółowości do poszczególnych grup zastosowań. W dalszej części niniejszego podrozdziału przedstawione zostały więc bariery jedynie dla kilku wybranych segmentów.

AGLOMERACJE MIEJSKIE – HOLISTYCZNE PODEJŚCIE DO ORGANIZACJI MIASTA

AMSTERDAM

Inteligentny Parking – podgląd wolnych miejsc parkingowych przez tablice informacyjne i aplikacje mobilne. Korzyści: redukcja emisji CO2, zmniejszenie korków, obniżenie kosztów operacyjnych za parkowanie (opłata przez aplikację). Inne aplikacje ułatwiające transport środkami publicznymi (Citimapper) lub umożliwiające miastu weryfikację uprawnień do parkowania w strefie (zdjęcia tablic rejestracyjnych).

Samochody elektryczne – miasto dysponuje flotą 300 aut. Otwieranie i zamykanie pojazdu odbywa się za pośrednictwem aplikację mobilnej, podobnie uruchamianie auta. Korzyści – zmniejszenie emisji CO2, zwiększenie mobilności oraz oszczędność czasu – samochód dostępny w ciągu 30 minut we wskazanym miejscu. Podobna usługa funkcjonuje dla elektrycznych skuterów.

Dystrybucja energii – projekt „Climate Street" – inicjatywa wśród 40 przedsiębiorców wspierających zrównoważony rozwój. Po dwóch latach pilotażu z wykorzystaniem 20 z 40 wytypowanych projektów odnotowano 8 % oszczędność energii co przekłada się na redukcję CO2 o 194 tony. Projekty dotyczyły m.in. wymiany lamp ulicznych na LED, wykorzystania inteligentnych liczników np. w celu sterowania klimatyzacją czy zastosowania elektrycznych pojazdów do wywozu śmieci.

BARCELONA

Inteligentny Parking – czujniki np. w okolicy Sagrada Familia. Korzyści: wzrost dochodów z opłat za parking 33%.

Inteligentne przystanki – dotykowe panele informacyjne z informacją o rozkładzie jazdy i dodatkowe informacje o atrakcjach turystycznych. Dodatkowo Wi-Fi, gdyż każdy przystanek jest podłączony do światłowodu i możliwość doładowania telefonu.

Oświetlenie uliczne – we współpracy z firmą Philips wymieniono 1100 latarni ulicznych zamieniając je na jednostki wielofunkcyjne. Oprócz oświetlenia o zmiennym natężeniu, lampy wyposażone są w hotspoty Wi-Fi, czujniki zanieczyszczenia oraz kamery monitoringu.

Gospodarowanie odpadami – czujniki sygnalizujące wypełnienia koszy, a nawet pnemumatyczny system odbioru za pomocą ssania z punktu centralnego przez sieć podziemnych rur.

Inne – inteligentne liczniki, wypożyczalnia rowerów, inteligentny systemem nawadniania parków i ogrodów, sieć czujników: zanieczyszczenie, hałas, przepływ mieszkańców, natężenie ruchu ulicznego.

Więcej: http://www.22barcelona.com/
https://arkinetblog.wordpress.com/2010/03/22/barcelona-will-vote-for-diagonal-redesign/

BERLIN

Autonomiczne mikrobusy – bezzałogowe mikrobusy dla ok. 12 osób poruszające się po ściśle określonych trasach. Pilotażowo testowano 1 pojazd w latach 2016–2017. Przewiduje się setki takich pojazdów za kilka lat.

Inne – inteligentne liczniki, ładowarki samochodów elektrycznych, czujniki zanieczyszczeń powietrza w celu identyfikacji przyczyn, czujniki wypełnienia pojemników na śmieci z komunikacją do aplikacji, budownictwo CUBE Berlin – inteligentny biurowiec.

Więcej: https://www.statistik-berlin-brandenburg.de/home.asp, http://www.5g-berlin.org/

SINGAPUR

Inteligentny transport – wykorzystanie autonomicznych pojazdów na mniej zatłoczonych ulicach, system kontroli sygnalizacji drogowej zasilany informacjami z czujników instalowanych pod skrzyżowaniami. Korzyści: dostosowanie zielonych świateł do potrzeb użytkowników ruchu, zmniejszenie emisji CO_2 w związku ze zwiększeniem płynności ruchu zmotoryzowanego.

Gospodarka odpadami – pneumatyczny system zasysania odpadów przez system rur. Pojemniki na śmieci wyposażone w czujniki co optymalizuje zarządzanie harmonogramem odbioru odpadów. Korzyści: optymalizacja czasowo-kosztowa: technologia pneumatyczna wykonuje zadanie w kilka minut vs. cały dzień pracy tradycyjnej ciężarówki; zwiększenie wykorzystania recyklingu.

AUCKLAND

W przyjętej strategii miasto stawia sobie za cel usprawnianie komunikacji cyfrowej w mieście, otwieranie dostępu do danych miejskich, wspieranie wspieranie innowacji proponowanych przez mieszkańców, upowszechnienie cyfrowej edukacji, usprawnienie transportu publicznego oraz zoptymalizowanie zużycia energii i gospodarki odpadami.

Rada miasta otwiera się na wdrażanie projektów od dostawców z sektora komercyjnego, w miejsce projektowania i tworzenia własnych rozwiązań, jednak nie zamyka się na tylko jednego, kompleksowego dostawcę.

Określono obszar testowy wdrażania nowych projektów z zakresu Smart City. Projekty przyjęte dziś do realizacji to: rewitalizacja rejonów portowych oraz budowa centrum innowacyjności w Wynyard.

Więcej: http://www.aucklandcouncil.govt.nz/EN/planspoliciesprojects/reports/Documents/aucklandprofileinitialresults2013census201405.pdf

BRISTOL

Otwarta platforma – kluczowy projekt „Bristol is Open" polega na otwarciu dostępu do danych publicznych pozyskiwanych z systemów zarządzających procesami w mieście.

Więcej: https://www.bristol.gov.uk/documents/20182/33191/Bristol+Econominc+Briefing+Sept+2016/e171a9ee – 8da6-427e-825d-3a06b7f48861)

WIEDEŃ

Inteligentny parking – rozwiązanie zawiera aplikację mobilną dla mieszkańców zintegrowaną z systemem pobierania opłat parkingowych

Inteligentny transport – aplikacja mobilna za pomocą, której można wykupić prawo przejazdu dowolnymi środkami komunikacji miejskiej.

Monitoring powietrza – system monitorowania jakości powietrza w czasie rzeczywistym.

Platforma IoT – Platforma agregująca dane płynące z rozwiązań inteligentnych i sensorowych, zarządzająca urządzeniami oraz otwierająca dostęp do aplikacji zewnętrznych.

Strategia miasta polega na sprzężeniu danych płynących z rozwiązań IoT w jednej warstwie agregacyjnej dla wykorzystania przez dowolne certyfikowane aplikacje. Jego włodarze kładą duży nacisk na innowacyjność w transporcie oraz ekologii.

Strategiczne

- Brak długofalowych strategii spowodowany skupieniem na typowych zakresach funkcjonowania miasta, bez eksplorowania nowych wyzwań i analizowania dostępnych rozwiązań, w szczególności w odniesieniu do mniejszych ośrodków miejskich.
- Brak spójnej strategii i wizji oraz koncepcji rozwoju Inteligentnych Miast na poziomie regionalnym i krajowym – brak rozwiązań systemowych, które ułatwiałyby wdrażanie koncepcji przez jednostki samorządowe.
- Brak ciągłości decyzyjnej między kadencjami, co ma przełożenie zarówno na warstwę strategiczną, jak i operacyjną.
- Brak zapisów dotyczących rozwoju Inteligentnych Miast w strategicznych dokumentach obejmujących rozwój miast.

Finansowe

- Brak środków finansowych na realizacje inwestycji w obszarze Inteligentnych Miast w perspektywie pilniejszych wydatków samorządowych w krótkim czasie. W tle są trudności w oszacowaniu zwrotu z inwestycji w krótkiej perspektywie czasowej. Z drugiej strony brak budżetów na działania w wyniku których korzyści wykraczają poza sferę danej jednostki samorządowej.
- Ograniczone możliwości finansowania projektów z różnych źródeł i w różnych modelach finansowania.
- Skomplikowane procedury pozyskiwania środków unijnych.
- Brak zalokowanych budżetów na szybkie ścieżki wdrożeń pilotażowych.
- Brak priorytetów na realizację projektów z zakresu Inteligentnych Miast i Budynków

Polityczne

- Brak ciągłości decyzyjnej wstrzymuje podejmowanie kluczowych analiz, definiowanie długofalowych wymagań, aplikowanie rozwiązań oraz inwestowanie w odważne technologie.
- Presja ekonomiczna tworzy wyzwanie, aby dostarczać więcej usług i rozwiązań mniejszym kosztem co wymaga nowoczesnego podejścia, nowych technologii oraz modeli biznesowych.

Technologiczne

- Wysoki poziom skomplikowania technologii (duży wybór, brak stabilności, brak standardów) stanowi istotną barierę zarówno na etapie wyboru rozwiązań, realizacji, procesu przetargowego i później wdrażania i integracji rozwiązań co wpływa na wolną adopcję technologii i projektów IoT.
- Brak wypracowanych standardów (czujniki, łączność, platformy) oraz mnogość rozwiązań powoduje problemy z interoperacyjnością.
- Istniejące systemy oraz infrastruktura – trudności z integracją.

Organizacyjne i proceduralne

- Problem z wewnętrznymi procedurami, które nie ułatwiają wdrażania projektów, które często dotykają wielu wydziałów.
- Brak koordynacji wdrażanych projektów, często są realizowane silosowo, niezależnie względem siebie.
- Brak horyzontalnego i holistycznego podejścia do zagadnienia harmonizacji procesów związanych z działaniem i wdrażaniem wertykalnych aplikacji Smart City.
- Poszczególne elementy infrastruktury miejskiej znajdują się w gestii różnych jednostek organizacyjnych co istotnie ogranicza koordynację działań.
- W wielu przypadkach brak klarownego właścicielstwa obszaru Smart City, w niektórych miastach powołani są koordynatorzy albo pełnomocnicy miasta zajmujący się przedmiotową tematyką ale również mają ograniczone pole działania.

Ludzkie

- Niska wiedza i świadomość kierunków ewolucji miast oraz w zakresie wdrażania i integracji nowoczesnych technologii. Dotyczy to zarówno zespołów po stronie administracji publicznej odpowiedzialnych za rozwój jak i odbiorców, tj. mieszkańców.
- Cyfrowe wykluczenie – brak umiejętności wykorzystania nowoczesnych technologii przez wybrane grupy społeczne.
- Bezpieczeństwo (szerzej na temat bezpieczeństwa w rozdziale 8).

Prawne

- Brak predefinicji ram innowacyjnych modeli biznesowych, w których inwestycje pokrywane są zarówno z budżetu samorządów, centralnych programów oraz firm sektora prywatnego. Samorządy wstrzymują angażowanie się w niestandardowe modele biznesowe w obawie przed brakiem regulacji. Bariery w zakresie dokonywania zakupów w modelu usługowym (*as a Service*), bądź w innych modelach (PPP).
- Brak rekomendacji dla ram procesu dialogu technologicznego.

- Ograniczenia we włączaniu inwestorów prywatnych w projekty publiczne przy otwieraniu innowacyjnych modeli biznesowych, jako źródło dochodu dla miasta.

Na poziomie poszczególnych obszarów zidentyfikowano ponadto następujące bariery:

Zarządzanie odpadami

- Firmy odpowiedzialne za gospodarowanie odpadami są bardzo konserwatywne we wdrażaniu innowacyjnych systemów, co wynika z braku świadomości o możliwych do uzyskania oszczędnościach. Krótki czas dostarczania usługi po przetargu (tj. 1-3 lata) wstrzymuje inwestycje w systemy, których zwrot z inwestycji pojawia się w dłuższej perspektywie.

- Trwałość czujników, odporność na wandalizm, efektywność kosztowa samych czujników i koszt wymiany (kosz na śmieci ma krótki okres pracy), przełamanie monopoli w wywózce śmieci, błędne odczyty wskutek składowania różnego rodzaju odpadów.

Inteligentne oświetlenie

- Infrastruktura oświetleniowa miejska należy do różnych aktorów (podmiotów), co uniemożliwia w praktyce wdrożenie zintegrowanych systemów, które byłyby zoptymalizowane kosztowo i technologicznie. Brak regulacji i predefinicji zakresu wdrożeń Inteligentnego oświetlenia, które technologicznie może otworzyć szeroką gamę aplikacji na tej samej infrastrukturze.

Inteligentne Miejskie Platformy Danych

- Brak rekomendacji technologicznych w zakresie standaryzacji platform operujących na danych publicznych powoduje pilotaże i wdrożenia rozwiązań silosowych (zamkniętych) – trudnych w rozwoju.

Inteligentne budynki

- Brak ulg podatkowych, które zmotywowałyby inwestycje w inteligentne zarządzanie budynkami, optymalizujące konsumpcje energii.

- Brak świadomości tzn. potencjalni użytkownicy nie są świadomi istnienia rozwiązań realnie zwiększających ich bezpieczeństwo.

Smart Parking

- Narażenie czujników na zniszczenie w zimie przez odśnieżanie, wandalizm, odpowiednia informacja dla kierowców o systemie i jak on działa.

Zanieczyszczenie środowiska

- Niechęć władz do otwartego i transparentnego pokazywania stanu zanieczyszczenia powietrza stąd niechęć do finansowania *Vending Telemetry*.

- Skala inwestycji, dodatkowe koszty wynikające ze zwiększenia mocy sygnałów (czujniki pod ziemią lub na poziomach głęboko poniżej poziomu gruntu, tzw. minus n), technologie czujników vs istniejące typy liczników.

Propozycje działań rządu

Wiele zastosowań z dziedziny Inteligentnych Miast jest w stanie przynieść namacalne korzyści, jednak jedynie w pełni holistyczne i zintegrowane podejście zapewni długotrwałe i wysokie wymierne korzyści. Pozwoli to połączyć systemy transportowe, transakcyjne, zarządzania energią oraz infrastruktury dla wyeksponowania największej wartości płynącej ze zintegrowanych aplikacji.

Wymaga to jednak podjęcia przez władze Polski szeregu działań stymulujących wdrożenie koncepcji Smart City w miastach, w szczególności:

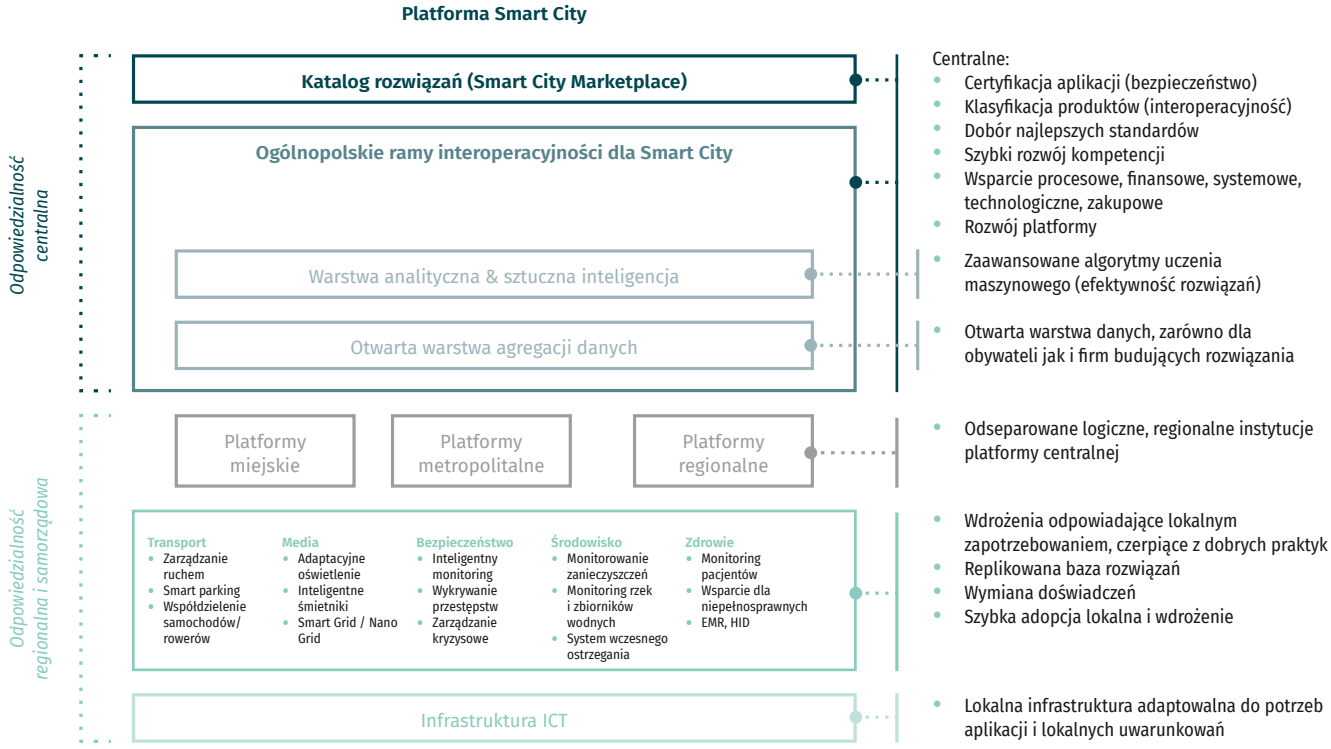
- Centralnej strategii usprawniającej wdrożenia i adresującej regionalne i samorządowe wyzwania, zintegrowanej ze strategią cyfryzacji Państwa. Strategia powinna zawierać mechanizmy dofinasowania wdrożeń i adresować interoperacyjność platform Smart City na wielu szczeblach w wymiarach takich jak: współdzielenie danych, interoperacyjność systemów komunikacji, interoperacyjność rozwiązań w zakresie bezpieczeństwa publicznego, ochrony zdrowia itp. Mechanizmy te powinny być oparte o ogólnopolskie Ramy Operacyjności Smart City, wsparte mechanizmami homologacji/certyfikacji usług i rozwiązań.

- Usystematyzowanych procesów, procedur dla realizacji projektów Smart City w Samorządach oraz centralnych kompetencji technologicznych. W szczególności wypracowanie wspólnie z organizacjami przedsiębiorców wzorców i dobrych praktyk wspierających zamawianie złożonych technologicznie rozwiązań jakimi są platformy usług Smart City.

- Stworzenie otwartego forum wymiany doświadczeń oraz informacji.

- Usunięcia wielu barier związanych z m.in. niską wiedzą i świadomością zarówno w zakresie technologii jak kierunków ewolucji miast, brakiem modeli opartych na Partnerstwo Publiczno-Prywatnym oraz ograniczeniach w wykorzystywaniu różnych modeli finansowania.

Mając na uwadze zidentyfikowane bariery ułatwienie adopcji technologii można by osiągnąć poprzez zcentralizowanie niektórych z usług (np. na poziomie regionu, województwa czy kraju) poprzez budowę jednej bądź kilku Zintegrowanych Platform Miejskich oraz stworzenie centralnego „Katalogu rozwiązań", zawierającego „gotowe" komponenty do poszczególnych obszarów. Istotne jest przy tym zagwarantowanie możliwości dostępu do tych samych technologii mniejszym miastom, czy gminom. Zarys koncepcji przedstawia rysunek na stronie 46.



Wraz z centralizacją wybranych funkcji konieczne jest również usunięcie wielu barier. Poniżej przedstawione zostały rekomendacje w tym zakresie:

Strategiczne i Finansowe

- Budowa programów wspierających samorządy na poziomie centralnym: wsparcie przy wyborze technologii i wdrażaniu, ale w szczególności współfinansowanie inicjatyw realizowanych przez samorządy.
- Zaangażowanie finansowych spółek Skarbu Państwa (PKO, PZU, BGK) w finansowanie i udzielanie gwarancji z wykorzystaniem spektrum instrumentów finansowych (np. leasing).
- Realizacja programów wspierających rozwój Inteligentnych Budynków – edukacja, ulgi.
- Analiza i rekomendacje technologiczne w dziedzinie budowania strategii wdrażania aplikacji i tworzenia platform danych.
- Umożliwienie alokacji budżetów na wdrożenia szybkiej ścieżki pilotażowej z puli środków samorządowych.
- Uwzględnienie Smart City w innych działaniach i dokumentach strategicznych – programy, plany obejmujące m.in. planowanie przestrzenne, długoterminowe plany rozwoju, plany gospodarki odpadami, polityka energetyczna, polityka rozwoju systemu wodno-kanalizacyjnego, polityka ochrony środowiska, programy związane z ochroną zdrowia oraz programy związane z strategicznymi planami budowy osiedli komunalnych).

Technologiczne

- Rozwój natywnej architektury chmurowej w celu wirtualizacji zasobów i umożliwienia szybkiego rozwoju i wdrażania nowych usług oraz aplikacji.
- Wsparcie rozwoju infrastruktury telekomunikacyjnej zarówno pod kątem Internetu Rzeczy jak i 5G, która otworzy całkiem nowe perspektywy.
- Wykorzystanie infrastruktury istniejącej w regionach – wskaźniki utylizacji tych zasobów są bardzo niskie, można więc założyć, że pewne zasoby obliczeniowe mogłyby być wykorzystane do realizacji celów związanych z budową infrastruktury pod kątem Inteligentnych Miast.

Organizacyjne i ludzkie

- Budowa sieci współpracujących ze sobą City Lab-ów, gdzie testowane byłyby różne rozwiązania we współpracy z dostawcami.
- Program szkoleń i edukacji w obszarze technologii Smart City dla samorządów.
- Inspirowanie i wsparcie inicjatyw samorządowych, których celem byłaby budowa centralnego repozytorium wiedzy i najlepszych praktyk.
- Stworzenie wzorców wdrażania projektów w strukturach miejskich (np. integracja i współpraca między wydziałami).

- Opracowanie wzorców służących do oszacowania opłacalności projektu w danym mieście, gminie, itp.

- Kontynuacja prac zainicjowanych przez Grupę Roboczą IoT – poszerzona i uszczegółowiona analiza barier we współpracy z głównymi interesariuszami i opracowanie szczegółowego planu działań.

- Uspójnienie prac realizowanych przez poszczególne ministerstwa i jednostki rządowe.

- Usprawnienie współpracy na linii rząd – Samorządy.

Prawne o charakterze ogólnym

- Zwiększenie elastyczności Prawa Zamówień Publicznych – wprowadzenie modeli usługowych, np. Smart Lighting as a Service oraz umożliwienie różnych form partnerstwa publiczno-prywatnego. Konieczność dokonania predefinicji ram procesu dialogu technicznego.

- Dokonanie analizy i predefinicji nowych modeli biznesowych wraz z rekomendacjami dla samorządów lokalnych.

- Określenie ram tworzenia samorządowych spółek celowych w dziedzinie innowacyjności i nadzoru nad innowacyjną infrastrukturą.

Prawne w zakresie wybranych obszarów

  - **Zarządzanie odpadami** – Propozycja legislacyjna: W art. 33 ustawy o odpadach sugeruje się wprowadzenie ust. 5 w proponowanym brzmieniu: „Minister właściwy do spraw środowiska w porozumieniu z ministrami właściwymi do spraw: budownictwa, planowania i zagospodarowania przestrzennego oraz mieszkalnictwa, gospodarki, łączności, informatyzacji, transportu, wewnętrznych określi w drodze rozporządzenia wdrożenie i utrzymanie inteligentnych systemów zarządzania odpadami w gminach, a w szczególności określi cele, wymagania, instalację, sposób pracy, finansowanie, utrzymanie systemów, zasady wyznaczania za pomocą systemu wysokości opłat dla mieszkańców oraz zasady przetwarzania danych osobowych w związku z korzystaniem z inteligentnego oprogramowania zarządzającego odpadami, kierując się zapewnieniem właściwego i efektywnego funkcjonowania technologii do zapewnienia zarządzania odpadami oraz ochroną praw i wolności obywateli.”.

  - **Inteligentne oświetlenie** Propozycja legislacyjna: W art. 18 ust. 1 ustawy z dnia 10 kwietnia 1997 r. Prawo energetyczne proponuje się nowe brzmienie pkt. 4: „planowanie i organizacja działań mających na celu racjonalizację zużycia energii i promocję rozwiązań zmniejszających zużycie energii na obszarze gminy, w szczególności poprzez wdrożenie i utrzymanie zintegrowanych systemów inteligentnego oświetlenia”;

  - **Zanieczyszczenie środowiska** Propozycja legislacyjna: W art. 90 ust. 5 ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska proponuje się nowe brzmienie pkt. 2: „wykorzystanie inteligentnych urządzeń do oceny poziomów substancji powietrza oraz agregacji i udostępniania informacji o tej ocenie”.

  - **Inteligetne budynki** – Ulga podatkowa na kształt ulgi termomodernizacyjnej.

Inne rekomendacje

- Zaangażowanie we współpracę z PKP w różnych aspektach:

  - Budowa strategii Smart City we współpracy z PKP – uwzględnienie infrastruktury kolejowej w koncepcji inteligentnego transportu.

  - Współpraca w budowie Inteligentnych Miast od zera (podejście *Greenfield*) tam, gdzie planowana jest budowa osiedli w ramach programu Mieszkanie Plus na terenach należących do PKP. To pozwoli na zebranie bezcennych doświadczeń i testowaniu różnych wariantów na żywym organizmie.

- Wsparcie pod kątem Inteligentnych Budynków

  - Program wsparcia lub wprowadzenie obowiązku posiadania czujników dymu i czadu.

  - Dalsze inwestycje w programy czystego powietrza. Wymiana kotłów na gazowe, redukcja wykorzystania kotłów na paliwo stałe. Weryfikacja możliwości dofinansowań oczyszczaczy powietrza w ośrodkach użyteczności publicznej (szkoły, przedszkola, żłobki, domy spokojnej starości).

  - Programy zwiększające edukację lub podnoszące poziom świadomości w zakresie włamań i samopomocy sąsiedzkiej.

  - Programy zwiększające edukację w zakresie oszczędzania energii.

  - Wsparcie dla programów preferencyjnych warunków opodatkowania w przypadku energooszczędnych budynków.

Rekomendowane projekty pilotażowe:

- Opracowanie architektury Platformy Smart City obejmującej funkcje centralne i regionalne. Budowa pilotażowej Miejskiej/Regionalnej Platformy Miejskiej.

- Budowa pilotażowego wdrożenia Inteligentnego Miasta dla wybranych osiedli budowanych w ramach programu Mieszkanie Plus.

- Budowa centralnego repozytorium wiedzy i najlepszych praktyk.

11

OCHRONA ZDROWIA

Mądry człowiek powinien wiedzieć, że zdrowie jest jego najcenniejszą własnością i powinien uczyć się, jak sam może leczyć swoje choroby.

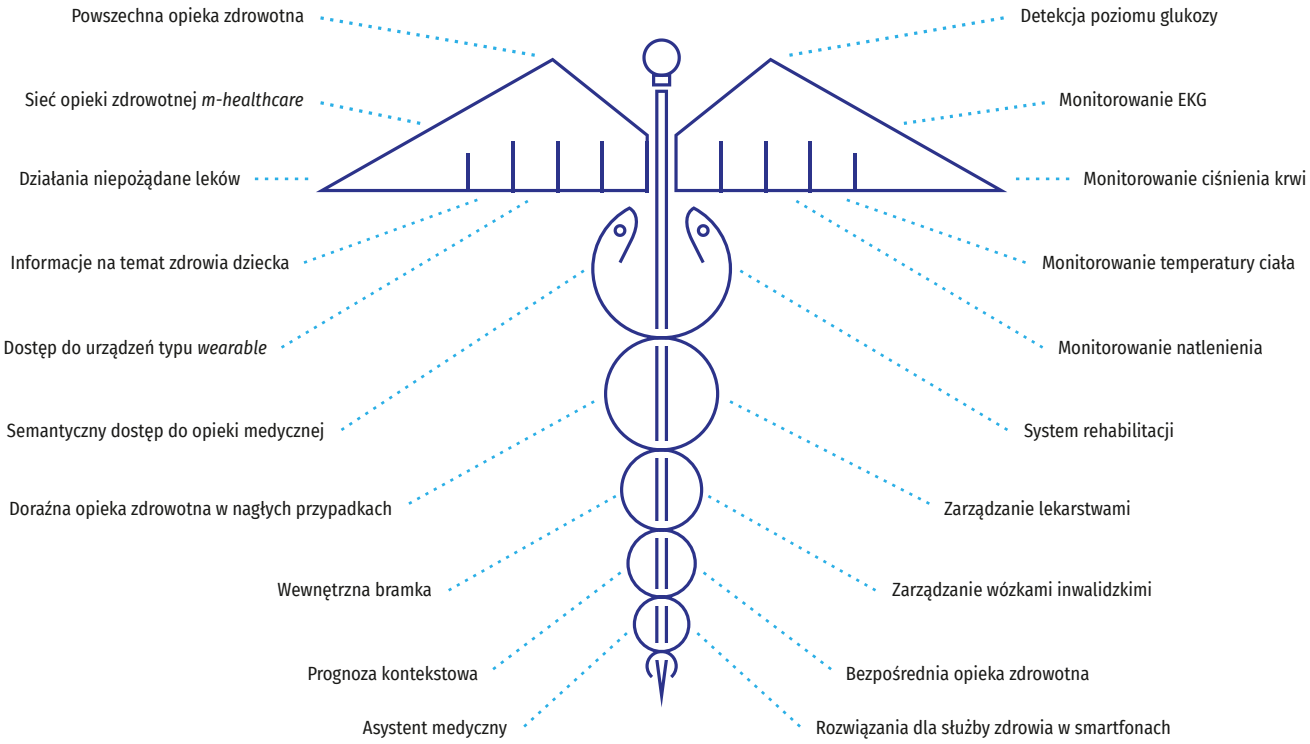
— *Hipokrates*

AUTORZY:
KRYSTIAN BIEŃ, POLPHARMA SP. Z O.O. – LIDER PODGRUPY
MICHAŁ JACKOWSKI, DSK KANCELARIA I LEX DIGITAL
MICHAL KOMAR, KANCELARIA PRAWNA D. DOBKOWSKI S P. K . STOWARZYSZONA Z KPMG W POLSCE
MICHAŁ KURASIŃSKI, POLPHARMA SP. Z O.O.
BARTOSZ NIEWIADOMSKI, GRUPA AVIVA
PIOTR TALAREK, TBT I WSPÓLNICY
PIOTR ZWOLIŃSKI, UCZELNIA ŁAZARSKIEGO

Ogólna charakterystyka branży

Ochrona zdrowia jest obecnie obszarem o potencjalnie bardzo dużej wartości dodanej dla polskiej gospodarki. Ministerstwo Zdrowia i Narodowy Fundusz Zdrowia są instytucjami odgrywającymi kluczową rolę na tym polu, dlatego tak ważne jest, by kierownictwo tych instytucji miało świadomość wartości płynącej z IoT w całym łańcuchu Business to Business to Consumer.

Wybrane serwisy i aplikacje Internet of Medical Things



Źródło: https://arxiv.org/ftp/arxiv/papers/1902/1902.00675.pdf („Characterizing IOMT/Personal Area Networks Landscape"; Effat University; Adil Rajput, Tayeb Brahimi)

Perspektywa rozwoju branży

Według raportu Allied Market Research[1], światowy rynek opieki dla Internetu Rzeczy osiągnie 136,8 miliardów dolarów do 2021 roku. Już teraz wykorzystuje się 3,7 miliona urządzeń medycznych.

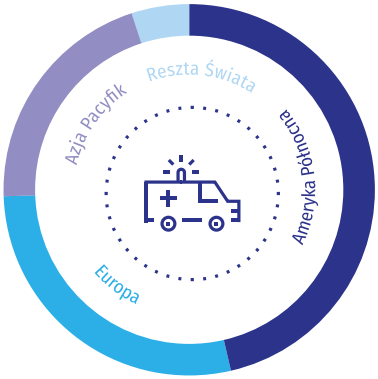
Potencjał rozwoju branży ochrony zdrowia w zakresie IoT obrazują następujące dane:

- 60% organizacji opieki zdrowotnej na całym świecie ma już technologię IoT w swoich ośrodkach,
- Do 2019 r. 87% dostawców usług opieki zdrowotnej wprowadzi rozwiązania IoT w usługach oferowanych w tym obszarze,
- Raport IDC przewiduje, że 40% organizacji opieki zdrowotnej będzie używać biosensorów z funkcją IoT do 2019 roku,
- 80% organizacji z obszaru opieki zdrowotnej zgłosiło wzrost innowacyjności dzięki wdrożeniu rozwiązań IoT,
- zgodnie z raportem[2] Aruba Network na temat stanu Internetu Rzeczy, 73% dostawców usług medycznych zdołało zmniejszyć koszty dzięki wykorzystaniu IoT,
- przewiduje się, że segment rynkowy tabletek inteligentnych osiągnie wartość 6,93 miliarda USD do 2020 roku,

1 https://www.alliedmarketresearch.com/iot-healthcare-market
2 Aruba Network

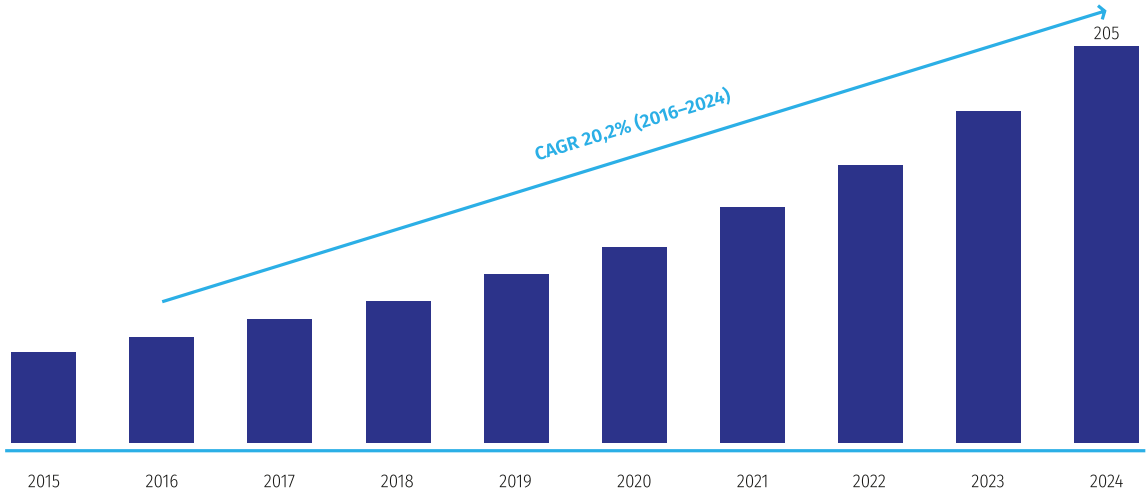
- najpopularniejsze rozwiązania IoT w organizacjach opieki zdrowotnej są wykorzystywane do monitorowanie i utrzymywania w dobrym stanie pacjentów – 73% natomiast do zdalnego nadzoru – 50%,
- raport IDC przewiduje, że do roku 2020 wydatki związane z Internetem Rzeczy osiągną 1,29 miliarda USD,
- wydatki globalne IoT wyniosą 1,4 miliarda USD do 2021 roku.

Rynek ochrony zdrowia w ujęciu kontynentalnym



Źródło: Variant Market Research

Światowy rynek IoT w ochronie zdrowia – stan aktualny i prognozy do 2024 r. (w miliardach USD)



Źródło: Variant Market Research

Zakres możliwego wykorzystania IoT

Prawidłowo zaimplementowane usługi diagnozowania i terapii zdalnej wykorzystujące rozwiązania IoT powodują obniżenie kosztów leczenia oraz podnoszą jakość usług medycznych.

Jednym z głównych aspektów jest fakt, iż wykorzystanie IoT w ramach zintegrowanego systemu ratownictwa medycznego znacząco podniesie przeżywalność oraz obniży koszty leczenia wynikające z następstw urazów, wypadków lub nagłego pogorszenia stanu zdrowia. Dodatkowo, prawidłowo zaimplementowane usługi diagnozowania i terapii zdalnej wykorzystujące rozwiązania IoT powodują obniżenie kosztów leczenia oraz podnoszą jakość usług medycznych, co prezentują następujące dane:

- Wizyty zdalne oparte o chmurowy system opieki i nadzoru wykorzystujący wszelkie narzędzia IoT (komputery personalne, urządzenia klasy smart, biosensory i struktura dostępowa) to nowy standard który powinien wypierać klasyczne rozwiązania. Tego chce dziś 70% populacji[3].
- Prawidłowo działające systemy cybernetyczne (chmurowe serwery medyczne oparte na nowoczesnych bazach ontologii) pozwolą na podniesienie jakości usług medycznych, ich unifikację i wykorzystanie efektu skali.
- Komunikacja telemedyczna i systemy IoT wykorzystujące roboty AI usprawnią ruch chorych i znacznie skrócą lub zlikwidują kolejki do lekarza (możliwe będzie lepsze wykorzystanie regionalne punktów dostępu medycznego).

3 raport PwC 12.2016 https://www.pwc.pl/pl/pdf/pacjent-w-swiecie-cyfrowym-raport-pwc.pdf

- Wobec perspektywy kosztów (pośrednich i bezpośrednich) związanych w chorobami cywilizacyjnymi (ChS-N i ch. nowotworowych) szacownych na 100 mld zł w 2030 r. zastosowanie IoT w diagnostyce, terapii i profilaktyce może przynieść znaczące oszczędności na każdym etapie[4].

- Stosowanie rozwiązań IoT przez pacjentów umożliwia bieżący nadzór nad terapią lekową pacjentów (ang. *medication adherence*), w tym w szczególności poprzez stosowanie bieżących przypomnień o potrzebie zażycia kolejnej dawki leku, instruktażu przy stosowaniu leków, godzeniu ze sobą różnego rodzaju terapii lekowych prowadzonych jednocześnie, wychwytywaniu interakcji pomiędzy stosowanymi lekami.

Dane gromadzone dzięki rozwiązaniom IoT służą lepszemu nadzorowi producentów leków i wyrobów medycznych nad stosowaniem produktów po ich wprowadzeniu do obrotu:

- Monitorowanie stosowania leków przez pacjentów poprzez rozwiązania IoT (np. *wearables*) pozwala na bieżące śledzenie działania leków oraz wychwytywanie ewentualnych działań niepożądanych.

- Wprowadzenie rozwiązań IoT w wyrobach medycznych umożliwia bieżący monitoring ewentualnych wad, błędów użytkowych, incydentów, które mają miejsce przy korzystaniu z wyrobów.

- Dane zbierane poprzez rozwiązania IoT stosowane w wyrobach medycznych pozwalają producentom podejmować niezbędne działania korygujące i zapobiegawcze, również w razie braku reakcji ze strony samych użytkowników wyrobów.

- Dane zbierane poprzez rozwiązania IoT stosowane w wyrobach medycznych stanowią uzupełnienie informacji gromadzonych w ramach nadzoru nad ich stosowaniem po wprowadzeniu do obrotu. Jako takie służą w szczególności do aktualizacji ustalenia stosunku korzyści do ryzyka stosowania danego wyrobu oraz przy usprawnianiu zarządzania ryzykiem.

Rozwiązania IoT wpływają również na wzrost dobrostanu starzejącego się społeczeństwa, poprawiając i wydłużając jakość życia pacjentów:

- Dane zbierane przez IoT (np. atestowane do użytku medycznego wearables) mogą przyczynić się do wczesnej kwalifikacji do badań przesiewowych w kierunku chorób otępiennych (AOTiM nie zaleca dziś wykonywania badań z uwagi na niską czułość dziś stosowanych testów; urządzenia z grupy IoT mogą prowadzić nieinwazyjny, stały monitoring stanu i zachowania osoby starszej).

- Czas, który zabiera wykonywanie czynności medycznych jest znacznie skrócony.

- Systemy cybernetyczne i liczne automatory mogą wykonywać czynności dotychczas wykonywane przez lekarza, jak również te, o których pamiętać musiał pacjent.

Bariery

Prawidłowa implementacja systemów i urządzeń IoT w ochronie zdrowia wymaga wielu zmian normatywnych, szczególnie w sferze ochrony konsumentów przed dyskryminacją, w zakresie określenia odpowiedzialności usługodawców i możliwości wykorzystania danych nieosobowych zbieranych w domenie publicznej.Konieczne jest również umożliwienie finansowania ze środków publicznych usług leczniczych wykorzystujących IoT.

Wykorzystanie IoT w systemie ochrony zdrowia (IOMT) jest we wczesnym stadium rozwoju. Zbyt wolno rośnie świadomość korzyści wynikających ze stosowania IoT wśród regulatorów, pacjentów, lekarzy i pracowników służby zdrowia.

W toku prac podgrupa zidentyfikowała następujące bariery dla branży:

- Brak jednego standardu, który definiuje komunikację zarówno pomiędzy urządzeniami IoT, jak i urządzeniami IoT z interfejsem usług zewnętrznych w obszarze zdrowia.

- „Inteligentne" implanty medyczne a bezpieczeństwo interfejsów komunikacji (zwłaszcza bezprzewodowych).

- Aspekty etyczne związane z danymi, które dostarcza technologia IoT.

- Zaufanie do technologii (różnice pokoleniowe).

- Brak finansowania ze środków publicznych świadczeń zdrowotnych udzielanych za pośrednictwem lub przy wykorzystaniu urządzeń telemedycznych – obecnie zakresem świadczeń gwarantowanych objęte są wyłącznie telekonsultacja kardiologiczna i geriatryczna[5].

- Ochrona danych osobowych oraz transgraniczny przepływ danych:

  - kwestią fundamentalną związaną z prawnymi aspektami medycznego IoT jest problematyka ochrony danych osobowych, w tym danych o stanie zdrowia,

  - w związku z tym, iż problematyka ta jest przedmiotem prac Grupy Roboczej ds. Ochrony Danych Osobowych,

4 http://www.zdrowepokolenia.org/uploads/news/Raport_kpmg.pdf?PHPSESSID=35qu106b0vup9p9i0m980sfkt5
5 http://www.nfz.gov.pl/aktualnosci/aktualnosci-centrali/telekonsultacja-kardiologiczna-i-geriatryczna-finansowana-przez-nfz,6758.html

powołanej przez Ministerstwo Cyfryzacji, nasz zespół świadomie zaniechał dokonywania szczegółowych analiz na ten temat, sygnalizując jedynie węzłowe problemy związane z tą materią.

- Węzłowe problemy odnoszące się do przetwarzania danych, które można zauważyć to:
  - problemy odnoszące się do danych osobowych przetwarzanych w systemach IoT reguluje RODO; jest to regulacja bardzo ogólna, która wymaga implementacji w dostosowaniu do sfery medycznego IoT,
  - ustawa wdrażająca RODO (ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO) nie zawiera przepisów przecyzujących zasady przetwarzania danych osobowych w sferze IoMT, w tym np. zasad współadministrowania danych przez dostawców urządzeń i odbiorców danych,
  - nie ma instrumentów regulujących konkretne reguły działania w sferze medycznego IoT – rekomendowane jest jak najszybsze przyjmowanie kodeksów branżowych i wprowadzenie mechanizmów certyfikacji,
  - brak mechanizmów umożliwiających zgodnie z art. 44–47 RODO przekazywanie danych osobowych do państw trzecich – rekomendowane jak najszybsze ich przyjęcie.
- Dyskryminacja związana z wykorzystaniem danych zebranych przy pomocy medycznego IoT
  - Dane zebrane za pomocą medycznych czujników i innych systemów medycznego IoT, bardzo precyzyjnie określające stan zdrowia, mogą być wykorzystywane dla celów nie tylko pozytywnych dla klienta – podmiotu danych, ale również w celach dyskryminujących, wykluczających. Już dziś w Stanach Zjednoczonych są dostępne plany ubezpieczeniowe, które w zamian za dostęp do urządzeń śledzących stan zdrowia oferują warunki premium. Problemy, które identyfikuje się w związku z tym to:
    - oferowanie tańszych usług w zamian za udostępnienie danych medycznych i biometrycznych na warunkach, które dla mniej zamożnych grup są jedynymi, na które osoby te stać, a „wybór" takiej usługi jest jedyną opcją,
    - karanie osób, których nawyki są postrzegane przez systemy IoT jako negatywne, mimo, że osoby te nie mają innych możliwości z uwagi na sytuację rodzinną czy finansową (bezsenność samotnego rodzica, uboga dieta osoby niezamożnej),
    - dyskryminacja cenowa przy wykorzystaniu danych medycznych wzmocniona metadanymi (data, znaczniki czasu i znaczniki geolokalizacji),
    - brak obiektywności czujnika – analizuje zawsze tylko pewien zakres danych, który może odbiegać od przeciętnej, ale w danym konkretnym przypadku i okolicznościach nie być szkodliwy dla podmiotu danych,
    - czujniki IoT mogą zbierać dane osobowe bez wiedzy i zgody podmiotów danych, a nadto generować duże strumienie danych ciągłych bez interwencji człowieka, łącząc się z innymi urządzeniami, poza kontrolą podmiotu danych,
    - nieprzejrzystość algorytmów może skutkować nieuczciwą kategoryzacją użytkowników.
- Dostrzegane jest, iż istniejące regulacje nie przeciwdziałają takiej dyskryminacji:
  - Ustawa wdrażająca RODO przewiduje np. szeroką możliwość zautomatyzowanego przetwarzania, w tym profilowania danych (także medycznych) oraz podejmowania decyzji wyłącznie na podstawie takich procesów.
  - Poza regulacjami sektorowymi brak jest regulacji przeciwdziałających opisanej wyżej dyskryminacji:
    - ustawa z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania określa obszary i sposoby przeciwdziałania naruszeniom zasady równego traktowania ze względu na płeć, rasę, pochodzenie etniczne, narodowość, religię, wyznanie, światopogląd, niepełnosprawność, wiek lub orientację seksualną; w zakresie medycznego IoT odnosi się zatem wyłącznie do niepełnosprawności,
    - również regulacje sektorowe są niepełne – np. wymieniona wyżej branża ubezpieczeniowa jest objęta zakazem dykryminacji cenowej, i to wyłącznie ze względu na płeć, ciążę i macierzyństwo – por. przykłady orzeczeń[6],
    - we współpracy z Rzecznikiem Finansowym należy przeanalizować problem dyskryminacji oraz dyskryminacji cenowej i opracować metody przeciwdziałania im.

6 http://www.ptpa.org.pl/site/assets/files/1029/wybrane_orzecznictwo_rownosc_kqed_info.pdf

OPASKI TELEMEDYCZNE W USŁUGACH MEDYCZNYCH I OPIEKUŃCZYCH

HTTP://SIDLY.EU/PL
POLSKA

PROBLEM

Starzejące się społeczeństwo i rosnąca liczba osób nie w pełni sprawnych fizycznie i umysłowo. Niskie poczucie bezpieczeństwa pensjonariuszy domów opieki. Ograniczone zaufanie do samorządów i fundacji. Czasochłonność działań związanych z wypełnianiem dokumentacji medycznej. Wysoka liczba zbędnych wizyt w gabinetach lekarskich, ostrych dyżurach czy wezwań pogotowia ratunkowego. Ograniczone środki finansowe, braki kadrowe niewystarczająca liczba placówek. Konieczność optymalizacji procesów w systemie opiekuńczo-medycznym.

ROZWIĄZANIE

Opaska teleopieki SiDLY – umożliwia automatyzację pomiarów medycznych, detekcję upadku z opcją zawiadamiania opiekuna o konieczności podjęcia reakcji, zawiera przycisk SOS, pomaga w zapobieganiu nieświadomym oddaleniom podopiecznych z ośrodka, przypomina o zażyciu leków, pozwala na zlokalizowanie użytkownika opaski.

KORZYŚĆ

Lekarze: redukcja czasu wypełniania dokumentacji – 60%; bezpośredni kontakt z pacjentem +29%; możliwość przyjęcia dodatkowych pacjentów.

Szpitale: zmniejszenie hospitalizacji o 35%; interwencje na „ostrym dyżurze” spadek o 53%; liczba „szpitalnych dni łóżkowych” spadek o 59%.

Samorządy: usprawnienie realizacji strategii opieki senioralnej, podniesienie jakości usług społecznych w samorządzie, zwiększenie atrakcyjności i innowacyjności polityki społecznej, zwiększenie atrakcyjności jednostek, jako miejsc zamieszkania dla osób niesamodzielnych, niepełnosprawnych, seniorów oraz wymagających stałego monitorowania. Opaski teleopieki SiDLY umożliwiają pozostanie w swoim środowisku seniorom, osobom mieszkającym samotnie i wymagającym wsparcia w codziennym funkcjonowaniu, bez konieczności przeprowadzenia się do placówki opiekuńczej.

Jednostki opiekuńcze: podniesienie jakości świadczonych usług, zwiększenie poczucia bezpieczeństwa podopiecznych oraz optymalizacja pracy opiekunów, zwiększenie konkurencyjności ośrodka.

REANIMATOR

APLIKACJA UŁATWIAJĄCA UDZIELENIE POMOCY OSOBIE Z NAGŁYM ZATRZYMANIEM KRĄŻENIA (NZK)
POLSKA

PROBLEM

W Polsce rocznie dochodzi do 40 000 zatrzymań krążenia. Wśród osób, u których doszło do NZK przeżywa w Polsce zaledwie 7%, podczas gdy w krajach skandynawskich ten współczynnik wynosi 40% (dane Europejskiej Rady Resuscytacji). W Polsce brak powszechnej wiedzy na temat udzielania pierwszej pomocy w takich przypadkach.

ROZWIĄZANIE

Aplikacja, zawierająca dwa główne moduły: Lokalizator automatycznego defibrylatora zewnętrznego (AED), który wskaże miejsce, gdzie znajduje się AED i doprowadzi do niego użytkownika najkrótszą drogą oraz „Wirtualny asystent", który poprowadzi użytkownika przez cały proces udzielania pomocy osobie nieprzytomnej. Aplikacja może być uzupełnieniem łańcucha przeżycia, na który składają się: rozpoznanie NZK, wezwanie profesjonalnej pomocy, wczesna defibrylacja, medyczne czynności ratunkowe prowadzone przez profesjonalistów.

KORZYŚĆ

Wzrost przeżywalności u osób z NZK, a tym samym zmniejszenie strat finansowych i kosztów społecznych śmierci osoby w wieku produkcyjnym. Te szacowane są przez ZUS na około 400 000 zł.
Poprawa przeżywalności o 1% to 400 zgonów mniej, co oznacza w długofalowej perspektywie oszczędności na poziomie 160 000 000 zł.
Wykorzystanie aplikacji (smartfonów) i pokrycia naszego kraju przez sieć LTE, jest nieodzownym elementem usprawniania działania systemu Państwowego Ratownictwa Medycznego w Polsce.

- brak jest również pełnej regulacji odnoszącej się do dyskryminującej odmowy świadczenia usługi – kwestia ta została uregulowana wyłącznie na poziomie art. 138 kodeksu wykroczeń i budzi wątpliwości (por. postanowienie SN z 14 czerwca 2018 roku, II KK 333/17 oraz stanowisko Rzecznika Praw Obywatelskich i Ministra Sprawiedliwości[7]).

- Wykorzystywanie urządzeń i systemów IoT dla celów realizacji praw użytkowników, przestrzegania prawa, a także bezpieczeństwa publicznego;
  - Usługi telemedycyny:
    - usługi diagnozowania i terapii na odległość, powodujące obniżenie kosztów oraz poszerzenie dostępności usług medycznych,
    - zalegalizowane zmianami z 2015 i 2018 roku, ale niewykorzystywane w pełny sposób,
    - nadal brak jest pewności, czy i kiedy określone usługi mogą być świadczone w drodze elektronicznej, a kiedy wymagają osobistej wizyty pacjenta (w 2018 roku zmieniono art. 42 ustawy o zawodach lekarza i lekarza dentysty. precyzując, iż usługa może być świadczona zdalnie po analizie dokumentacji medycznej pacjenta, art. 8 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta wymaga zachowania należytej staranności z zachowaniem wymagań fachowych z odrębnych przepisów),
    - brak jest regulacji, które umożliwiałyby refundowanie usług telemedycyny przez NFZ.
  - Brak jest jakichkolwiek prawnych regulacji, które umożliwiałyby strukturalne wykorzystanie systemów i urządzeń IoT dla prowadzenia programów:
    - Badań przesiewowych;

7 https://www.rpo.gov.pl/pl/content/rzecznik-praw-obywatelskich-wyjasnia-jakie-przepisy-obliguja-do-interwencji-w-sprawie-dyskryminacji

- Badań epidemiologicznych;
- Wykorzystywania Big Data w działalności medycznej;
- Całość działań, które są podejmowane w tej sferze, stanowi inicjatywę podmiotów prywatnych. Dane pozyskiwane przez te podmioty nie stanowią domeny publicznej nawet po ich anonimizacji i nie mogą być wykorzystywane dla celów profilaktyki i zwalczania epidemii.

  - Brak jest jakichkolwiek przepisów, które stymulowałyby pozytywne zachowania w sferze zdrowia, a które mogłyby być monitorowane przy pomocy systemów i czujników IoT (przykładem takich regulacji może być sec. 10408 tzw. Affordable Care Act (Obamacare)[8]

- Odpowiedzialność podmiotów wykorzystujących usługi i systemy IoT:
  - Polskie przepisy nie zawierają żadnej regulacji odnoszącej się do odpowiedzialności producenta lub usługodawcy w zakresie IoT – kwestię tę reguluje szereg przepisów rozproszonych w kodeksie cywilnym, RODO, ustawie o świadczeniu usług drogą elektroniczną.
  - Do najważniejszych problemów, które należy zasygnalizować zaliczamy:
    - rozmyta odpowiedzialność, gdy usługi są łączone, a dane przekazywane wielu podmiotom – niejasne, kto jest podmiotem odpowiedzialnym za naruszenie,
    - brak jasnej regulacji odnoszącej się do odmowy świadczenia usługi,
    - brak jasnej regulacji dotyczącej kontynuacji świadczenia usługi – długości wsparcia, zakresu licencji kolejnych wersji oprogramowania,
    - brak regulacji dotyczących zakresu zabezpieczenia wymaganego w urządzeniach IoT – to użytkownik jest administratorem danych przetwarzanych za ich pośrednictwem, odpowiedzialnym za ich należyte zabezpieczenie,
    - niewystarczające regulacje odnoszące się do informacji o produkcie, danych przetwarzanych za jego pośrednictwem i skutkach wykorzystywania,
    - brak wymagań odnoszących się do gwarancji, odpowiedzialności, szyfrowania etc., zwłaszcza w regulacjach między przedsiębiorcami, gdzie możliwe jest niemal całkowite wyłączenie odpowiedzialności usługodawcy, a z drugiej strony użytkownik sam może ingerować w produkt (uzupełniać danymi, modyfikować, łączyć z innymi ekosystemami),
    - brak regulacji umożliwiających poznanie algorytmów przetwarzania w celu zapewnienia ich dokładności i rozliczalności.
  - Jest świadomość, iż organy UE pracują nad nową regulacją o cyberbezpieczeństwie[9].
- Wykorzystanie urządzeń IoT w toku postępowań:
  - Nie ma przepisów, które regulowałyby wykorzystanie danych zawartych w urządzeniach IoT dla celów postępowań sądowych i administracyjnych – podlegają ogólnym przepisom dowodowym.
  - Dostrzegane problemy:
    - brak dostępności tych danych, zwłaszcza gdy usługodawca przetwarza dane poza granicami kraju – strona polskiego postępowania, a nawet sąd, będzie miał istotne problemy w uzyskaniu dostępu do tych danych, zwłaszcza gdy są zaszyfrowane,
    - brak jasnych procedur, na podstawie których można zweryfikować prawdziwość i dokładność tych danych – brak dostępu do algorytmów, brak biegłych dysponujących odpowiednią wiedzą, brak możliwości przesłuchania producenta w charakterze biegłego,
    - preferencja innych źródeł dowodowych (zeznań osób, opinii biegłych),
    - ograniczenia techniczne polskich sądów – brak możliwości włączenia danych do akt postępowań (zwłaszcza gdy nie można ich zapisać na płycie lub nośniku USB), brak możliwości odtworzenia po odłączeniu od IoMT (ang. *Internet of Medical Things*).

8 http://housedocs.house.gov/energycommerce/ppacacon.pdf
9 https://www.consilium.europa.eu/pl/policies/cyber-security/

Propozycje działań rządu

Rekomendujemy następujące działania prawne:

- Uzupełnienie zapisów ustawy o systemie informacji w ochronie zdrowia, o adekwatne do aktualnego rozwoju technologii zapisy dotyczące telemedycyny oraz IoMT.
- Zmianę aktów prawnych, szczególnie w sferze ochrony konsumentów przed dyskryminującym ich wykorzystaniem, odpowiedzialności usługodawców, jak również zmian umożliwiających finansowanie usług leczniczych wykorzystujących IoT ze środków publicznych i wykorzystanie nieosobowych danych zebranych w tych procesach w domenie publicznej.
- Umożliwienie dodania do elektronicznej dokumentacji pacjenta danych pochodzących z wykorzystywanych przez niego wyrobów medycznych (np. termometr, ciśnieniomierz, spirometr).
- Przyjęcie pełnej regulacji, która przeciwdziałałaby dyskryminującemu wykorzystaniu danych, w tym danych medycznych pozyskiwanych przy pomocy systemów IoT.
- Wprowadzenia regulacji umożliwiających świadczenie usług telemedycznych za pośrednictwem IoT z wykorzystaniem Big Data i bez ingerencji lekarza, w szczególności, gdy jest ona zbędna (np. programy screeningu osób zdrowych, zbieranie danych ze względów epidemiologii).
- Wprowadzenie regulacji umożliwiających wykorzystanie danych anonimowych zebranych przez podmioty prywatne przez publiczną służbę zdrowia.
- Aktywne włączenie się organów w prace nad regulacją unijną.
- Podjęcie prac nad spójnym z regulacją unijną akcie prawnym regulującym odpowiedzialność producentów i usługowców medical IoT (wzorem może być projekt amerykańskiego aktu prawnego – Internet of Things (IoT) Cybersecurity Improvement Act of 2017[10]).

Rekomendujemy następujące działania pozaprawne:

- Projekty kształcenia uczniów szkół w zakresie prowadzenia zdrowego trybu życia – przekazywanie za pośrednictwem młodzieży informacji ich rodzicom / dziadkom (akcje „opowiedz o tym swoim rodzicom") o urządzeniach / aplikacjach możliwych do zastosowania w diagnostyce chorób / monitorowania stanu zdrowia.
- Zaleca się przygotować plany edukacji społeczeństwa w zakresie używania urządzeń / systemów wspierających procesy ratownictwa medycznego.
- Należy przygotować plany edukacji przedstawicieli zawodów medycznych, aptecznych oraz pacjentów w zakresie używania urządzeń IoT oraz możliwościach ich zastosowań.
- Stosowanie zachęt oraz szkoleń dla lekarzy do korzystania z danych udostępnianych im przez pacjentów, w tym danych pochodzących z urządzeń / aplikacji do monitorowania stanu zdrowia.
- Upusty w składce na ubezpieczenie zdrowotne / upusty w cenach leków refundowanych dla osób stale monitorujących stan swojego zdrowia i przekazujących dane o stanie zdrowia do elektronicznej dokumentacji medycznej.
- Umożliwienie finansowania usług telemedycznych ze środków publicznych.
- Wprowadzenie jasnych procedur, które dookreśliłyby dopuszczalność świadczenia usług telemedycznych.
- Uruchomienie przez Ministerstwo Zdrowia projektów pilotażowych wykorzystujących możliwości, jakie daje technologia IoT. Rozwiązania, które dają największe korzyści z punktu widzenia: oszczędności, wykorzystania posiadanej infrastruktury, skuteczności profilaktyki i leczenia, bądź mające największy potencjał wykorzystania w innych usługach świadczonych przez państwo, powinny być w dalszej kolejności realizowane na większą skalę.
- Utworzenie publicznego funduszu celowego (np. w ramach NFZ) na wsparcie (częściowe finansowanie) wdrażania polskiej myśli technicznej – opracowanych w Polsce rozwiązań IoT dla sektora medycznego.
- Należy wprowadzić zasady certyfikacji urządzeń, aplikacji, systemów wspierających proces udzielania pierwszej pomocy, kwalifikowanej pierwszej pomocy i medycznych czynności ratunkowych.
- Wybrane Programy Polityki Zdrowotnej Ministerstwa Zdrowia (np. profilaktyczne) powinny być uzupełnione o możliwość promocji i wykorzystywania rozwiązań IoT np.:
  - Program Profilaktyki i Leczenia Chorób Układu Sercowo-Naczyniowego (POLKARD na lata 2017–2020),
  - Kompleksowej Opieki Nad Osobami z Niewydolnością Serca (KONS),

10 https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?q=%7B%22search%22%3A%5B%22S.1691%22%5D%7D&r=1

w celu możliwie bezinwazyjnego monitorowania stanu zdrowia i/lub aktywności osób zakwalifikowanych do grup ryzyka (z jednoczesną redukcją wizyt w placówkach szpitalnych i/lub ambulatoryjnych). Dotyczy to w szczególności osób starszych, często pozbawionych bieżącej opieki bądź pacjentów geriatrycznych (po 70 r.ż.), gdzie celem systemu ochrony zdrowia jest zapewnienie możliwie długotrwałego dobrostanu w warunkach domowych;

- Wdrożenie IoT w opiece senioralnej, finansowanej przez samorządy, usprawni ich działanie i zwiększy sprawność przy utrzymaniu budżetów operacyjnych (*OPEX – operating expenditures*);
- Usługi dostarczane przez dostawców powinny być zgodne z protokołem HL7 (Polskie Stowarzyszenie HL7);
- Przesył danych telemetrycznych używanych na potrzeby medycznych czynności ratunkowych powinien być wyłączony z konieczności uzyskania zgody na przetwarzanie szczególnych danych osobowych;
- Warto wprowadzić priorytetyzację kanałów komunikacji dla urządzeń, aplikacji, systemów działających w trybie „na ratunek”;
- Warto uwzględnić w SWDRM (System Wspomagania Dowodzenia Ratownictwem Medycznym) opcji przesyłania strumienia video z miejsca zdarzenia do dyspozytorni / zespołu ratunkowego;
- Zaleca się utworzyć krajowy rejestr urządzeń AED (wymóg formalny). Takimi informacjami mógłby być zasilony zbiór danych w GUGiK. Repozytorium stanowiłoby źródło dla obecnych i przyszłych rozwiązań informatycznych;
- Zaleca się utworzyć krajowy rejestr osób przeszkolonych z udzielania KPP (kwalifikowana pierwsza pomoc) użyteczny w przypadku wystąpienia sytuacji kryzysowej;
- Zaleca się wprowadzenie i zastosowanie standardu szerokiego zgłaszania działań niepożądanych zarówno przez przedstawicieli zawodów medycznych, jak i pacjentów;
- Można rozbudować system profilaktyki pierwotnej i wtórnej wielu chorób i w ten sposób obniżać ryzyko choroby powodującej obniżenie jakości życia, absencje w pracy i inwalidyzację;
- Diagnostyka oparta (lub wsparta) rozwiązaniami IoT może wesprzeć aktualizację i tworzenie przez Ministerstwo Zdrowia Map Potrzeb Zdrowotnych;
- Zaleca się umożliwienie wykorzystanie danych zbieranych przez IoT w procesie zgłaszania działań niepożądanych oraz na potrzeby epidemiologii;
- Warto zastanowić się nad dobieraniem parametrów medycyny spersonalizowanej dla indywidualnych pacjentów co pozwoli na optymalne ustalenie profilu zdrowia i lepszego dłuższego życia. To jest ustalane i potem kontrolowane przez biosensory;
- Zastosowanie rozwiązań IoT, finansowanych na poziomie krajowym (programy profilaktyczne) i samorządowym (opieka senioralna) zwiększy bezpieczeństwo, dobrostan i niezależność ludzi starszych, zwłaszcza tych:
  - nie posiadających stałej opieki domowej,
  - będących w stanie zdrowia nie wymagającym hospitalizacji, poniżej 70 oku życia,
  - nie borykających się z wielochorobowością (np. zespół słabości, depresja, parkinsonizm, otępienie, upadki).

12

INTELIGENTNE OPOMIAROWANIE

Najlepszym sposobem na przewidzenie przyszłości jest jej kreowanie.

— *Abraham Lincoln*

AUTORZY:
KRZYSZTOF WADAS, GRUPA CYFROWY POLSAT – LIDER PODGRUPY
JERZY GREBLICKI, AIUT SP. Z O.O.
RADOSŁAW KOTEWICZ, COMARCH S.A.
RAFAŁ KOWALSKI, DIEHL METERING SP. Z O.O.

Ogólna charakterystyka branży

W branży rośnie świadomość korzyści z połączenia rozwiązań IoT z AI, BI i Big Data. Coraz więcej firm buduje swoje własne kompetencje w tych obszarach – powstają pierwsze pilotażowe wdrożenia, które realnie wykorzystują technologie IoT (urządzenia IoT, aplikacje pod IoT i transfer danych w nowych technologiach transmisji). Rośnie także świadomość klientów końcowych dotycząca możliwości wykorzystywania danych do optymalizacji swoich wydatków domowych (wiem, jak konsumuję dziennie/miesięcznie energię elektryczną, wodę lub gaz). Dane zbierane z mierników IoT w sektorach branżowych będą z czasem udostępniane online na smartfonach klientów końcowych.

Polskie firmy z sektora analizują w testowych wdrożeniach (trial) dostępne technologie transmisji – NB-IoT, CAT-1M, LoRaWAN, Sigfox – i analizują je pod kątem ich przydatności dla przyszłych wdrożeń. Dane z zagranicy pokazują, że globalnie wdrożenia IoT w sektorze energetyki i szeroko pojętych utilites wzrosło do 36% w 2019[1]. W Polsce możemy śmiało powiedzieć, że lata 2019–2021 będą rozwojowe w obszarze IoT. W tych latach pojawią się na rynku pierwsze duże wdrożenia.

Wyzwania dla branży to: zabezpieczenie się przed nadmierną regulacją, która wpływa na ograniczenie polskiej innowacyjności w tym zakresie, przestarzała sieć energetyczna oraz niezrozumienie korzyści użycia nowych technologii w samorządach (konieczne jest wdrożenie i opublikowanie „Polskiego Leksykonu Pojęć Internetu Rzeczy"), uzależnienie decyzji o inwestycjach w usługi i produkty od dostępności infrastruktury komunikacyjnej (brak stymulacji państwa do budowania usług operatorskich / rozwoju infrastruktury poprzez realne zainteresowanie projektami IoT w spółkach z udziałem Skarbu Państwa).

Perspektywa rozwoju branży

W chwili obecnej widzimy bardzo dużą szansę na wzrost udziału sektora IoT i AI w PKB w Polsce. W tym celu wymagane jest wsparcie budowania polskich, ukrytych globalnych championów. Referencje, nawet z małych projektów w Polsce, są trampoliną dla ekspansji za granicą. Należy tutaj podkreślić, że celem nie jest zdominowanie rynku lokalnego, celem jest działanie globalne (UE, USA, rynki azjatyckie i Bliskiego Wschodu), które przyniesie wzrost konkurencyjności polskich firm, co w dalszej perspektywie przekłada się na wzrost PKB kraju. W Polsce funkcjonują już rodzime firmy, które z powodzeniem prowadzą taką ekspansję w obszarze IoT.

Polska ma również szansę zaistnienia w Europie jako swego rodzaju Hub IoT, który może dostarczać urządzenia IoT, aplikacje do usług IoT oraz certyfikacje urządzeń polskich i zagranicznych IoT na rynek krajów UE (szybsza i skuteczniejsza certyfikacja produktów w Polsce, które potem sprzedawane są w UE). Z opłat za taką certyfikację urządzeń IoT pod branże energetyczne i inteligentne mierniki będą nowe przychody. Ponadto należy założyć otwartość na nowe technologie i standardy, przy jednoczesnej transparencji rozwiązań i otwartości przyjętych rozwiązań technicznych w tym protokołów. Otwarcie na nowe technologie, poparte gromadzeniem doświadczeń i zarządzania wiedzą, umożliwi stworzenie „Księgi dobrych praktyk dla IoT" co przełoży się na przyspieszenie wdrożeń w obszarze publicznym, przemyśle i na rynku konsumenckim. Zmniejszone zostaną ryzyka techniczne, przedstawiona skuteczna metodologia prowadzenia projektu IoT, proponowany plan jakości z podziałem odpowiedzialności dostawca – kupujący, zaproponowane będą minimalne (nieprzewymiarowane) wymagania co do bezpieczeństwa.

1 Vodafone IoT Barometr 2019

Zakres możliwego wykorzystania IoT

Praktyka i statystyki z zagranicy pokazują, że wdrażanie inteligentnych mierników jest realizowane głównie po to, aby mierzyć zużycie (67% wdrożeń zagranicą) oraz do monitorowania infrastruktury firm – 75% wdrożeń używa tych rozwiązań do kontrolowania bezpieczeństwa.

W Polsce również firmy z obszaru utilities widzą korzyści IoT – przykład: wodociągi chcą korzystać z rozwiązań IoT, aby szybko wykrywać wycieki (duże wypływy wody z uszkodzonej instalacji). Wdrożenie IoT daje korzyści dla firm (optymalizacja procesów, szybsze przesyłanie danych i ich analiza, monitorowanie bezpieczeństwa sieci), ale również dla klientów końcowych (większa wiedza na temat konsumpcji wody, energii lub gazu). Należy zaznaczyć, że wdrożenie zdalnego odczytu liczników rozszerza znacząco możliwość implementacji opomiarowania na obiektach, w których dotychczasowa technologia rejestratorów była nieopłacalna ekonomicznie. Dobrym przykładem jest opomiarowanie gazomierzy odbiorców indywidualnych – w taryfach W1–W3 poprzez zdalny odczyt wskazań gazomierzy domowych, obsługę gazomierzy przedpłatowych oraz obsługę gazomierzy windykacyjnych. Ponadto możliwe jest opomiarowanie ciśnienia w sieci dystrybucyjnej oraz monitorowanie końcówek podsieci (najdalszy odbiorca) w celu oceny jakości dostarczanej usługi (dostępność gazu o odpowiednim ciśnieniu). Rozwiązania takie mogą przyczynić się do poprawy bezpieczeństwa poprzez identyfikację awarii dzięki monitorowaniu przekroczenia progów alarmowych ciśnienia roboczego w sieciach transportujących (średnie i wysokie ciśnienie) oraz w zakresie opomiarowanie domowych czujników obecności gazu / tlenku węgla u użytkowników końcowych. Rozwój technologii IoT może być też elementem ułatwiającym realizację rozwiązań iskrobezpiecznych (pracujących w strefach zagrożenia wybuchem) – z uwagi na niski pobór energii rozwiązań IoT, a tym samym efektywniejsze niż dotąd wykorzystanie bateryjnych źródeł energii.

Ponadto infrastruktura oparta na dedykowanych rozwiązaniach telekomunikacyjnych dla potrzeb opomiarowania (SigFox, LoRa) może być wykorzystywana w szerszym zakresie jako platforma komunikacji masowej urządzeń IoT, alternatywna do obecnie dostępnych (GSM, LTE).

NRW – **Non-Revenue Water** – Woda niezafakturowana

Pod pojęciem wody niezafakturowanej rozumiemy różnicę pomiędzy objętością wyprodukowanej i wtłoczonej do sieci wody a objętością, która w procesie dystrybucji nie została dostarczona do klienta i tym samym nie została ona w żaden sposób zafakturowana. Składać się na to może wiele czynników takich jak wycieki czy nielegalne pobory wody, ale również prowadzone przez przedsiębiorstwa prace technologiczne na sieci.

SMART METERING W WODOCIĄGACH – WDROŻENIE W MPWIK W PIEKARACH ŚLĄSKICH

POLSKA

PROBLEM

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w Piekarach Śląskich chciało na bieżąco monitorować swoje wodomierze oraz zredukować koszty transmisji danych na terenie miasta.

ROZWIĄZANIE

Projekt oparty na wykorzystaniu transmisji LoRa opracowany przez polską firmę AIUT z Gliwic. Działające od lipca 2018 r. i wciąż rozwijane wdrożenie w Miejskim Przedsiębiorstwie Wodociągów i Kanalizacji Piekary Śląskie, jest systemem do zdalnego odczytu wodomierzy na terenie miasta. System składa się z anten sieci LoRa Kerlink, tworzących wydzieloną sieć dla potrzeb miasta. Zapewniają odczyt docelowo ponad 6500 wskazań wodomierzy na terenie miasta.

KORZYŚĆ

Obniżenie kosztu transmisji danych na terenie miasta oraz minimalizacja strat. Zastosowanie odczytów godzinnych czy codziennych zgłoszeń urządzeń pozwala na szybkie wynajdywanie wycieków u klientów lub wykrycie bezprawnego cofania licznika wody. Przy zastosowaniu sieci LoRa pokrywającej miasto, można w łatwy sposób dołączyć opomiarowanie stref i ciśnień w sieci wodociągowej. Zainstalowane w całym mieście anteny mogą też bezproblemowo łączyć się z innymi typami urządzeń, przykładowo służącymi do opomiarowania ciepłomierzy czy do kontroli ilości wolnych miejsc parkingowych.

Na podstawie ustawy Prawo Wodne z dnia 20 lipca 2017 roku, utworzono Państwowe Gospodarstwo Wodne Wody Polskie będące centralną instytucją zarządzającą krajową gospodarką wodną, natomiast Krajowy Zarząd Gospodarki Wodnej i regionalne zarządy gospodarki wodnej stały się jednostkami organizacyjnymi Wód Polskich.

W związku z powyższym, gwałtownie wzrosło zainteresowanie przedsiębiorstw gospodarki wodnej, rozwiązaniami służącymi minimalizacji ponoszonych przez nie kosztów produkcji wody niezafakturowanej. Aby umożliwić ich obniżenie, niezbędne jest monitorowanie i bilansowanie zużycia wody w strefach DMA (District Metered Area), ale również wymagana jest znajomość min. topologii sieci oraz panującego w niej ciśnienia.

Komunikacja IoT może w bardzo wyraźny sposób przyśpieszyć wdrażanie przez polskie przedsiębiorstwa gospodarki wodnej strategii NRW oraz mieć istotny wpływ na wzrost jej efektywności (chociażby poprzez zapewnienie częstszego pozyskiwania i przekazywania do dalszego procedowania danych pomiarowych bez konieczności inwestowania oraz utrzymywania własnej infrastruktury komunikacyjnej przez przedsiębiorstwa związane z branżą wodociągową).

Bariery

Przeregulowanie jest największym zagrożeniem dla sektora energii i usług komunalnych. Regulacje powinny zapewniać otwartość, eliminować ograniczenia i równocześnie nie dopuszczać do tworzenia monopoli, ograniczeń w tworzeniu nowych standardów komunikacyjnych, blokowania wprowadzania nowych technologii. Obecnie w branży

SMART METERING – ROZWIĄZANIE WYKORZYSTUJĄCE SIEĆ NB-IoT

EMIRATY ARABSKIE

PROBLEM

Powszechny problem w Zjednoczonych Emiratach Arabskich stanowi dostęp do zasobów wody pitnej, co wymaga racjonalnej gospodarki infrastrukturalnej. Lokalne przedsiębiorstwo wodociągowo-energetyczne w Dubaju posiada znaczną ilość liczników wody rozmieszczonych na obszarze całego kraju, 2–8 metrów pod powierzchnią ziemi. Tradycyjne mierniki czy to wody, energii elektrycznej, gazu lub ciepła wymagają manualnego odczytu danych, co generuje wysokie koszty utrzymania oraz powoduje braki w bieżącej informacji na temat przepływów i alarmów.

ROZWIĄZANIE

Zdalny odczyt liczników. Na początku roku 2019 w partnerstwie z lokalnym operatorem komórkowym przedsiębiorstwo wodociągowe zainstalowało 500 modułów M-Bus – NB-IoT firmy COMARCH. Dzięki wykorzystaniu standardu komunikacji NB-IoT urządzenie zapewnia zwiększony (w porównaniu do innych technologii GSM) zasięg sieci oraz niskie zużycie energii elektrycznej, co pozwala do 12 lat pracy na baterii. Dzięki obudowie IP68 urządzenie jest odporne na zalanie podczas gwałtownych deszczy na pustyni.

KORZYŚĆ

Obniżenie kosztów generowanych przez manualny odczyt liczników, wykonywany przez pracowników. Monitorowanie stanu sieci wodociągowej w czasie rzeczywistym pozwala na wczesne zapobieganie awariom sieci wodociągowej. Rozwiązanie nie generuje dodatkowych kosztów, gdyż nie wymaga wymiany istniejącej infrastruktury – moduł Comarch M-Bus – NB-IoT zapewnia bezprzewodową komunikację dalekiego zasięgu.

IoT trwa prawdziwa rewolucja technologiczna – im mniej ograniczeń prawnych lub proceduralnych, tym szybciej można komercjalizować nowe technologie, tworząc w oparciu o nie dojrzałe rozwiązania. W tym obszarze należy korzystać z doświadczeń podejścia USA w zakresie swobody prowadzenia działalności gospodarczej (*corporate freedom*).

Podgrupa stoi na stanowisku, że z ostrożnością należy podchodzić do centralizowania procesów związanych z dostępem do danych. Ograniczony czasochłonnymi procedurami dostęp do informacji może znacząco ograniczyć innowacyjność branży i motywację do szybkiego reagowania na zmiany.

Kolejną barierą jest również sama dostępność usług komunikacyjnych w domenie publicznej lub B2B. Popularyzacja dostępności NB-IoT lub LTE CAT-M uzależniona jest od decyzji strategicznych i inwestycyjnych istniejących operatorów telekomunikacyjnych. Aktualnie niedostępne są komercyjne taryfy dla tych usług co w zasadniczy sposób ogranicza możliwość budowania modeli ekonomicznych oferowania usług, a tym samym inwestycji w rozwój aplikacji sprzętowych. Wydaje się, że wśród przyczyn takiego stanu rzeczy jest brak porozumienia pomiędzy operatorami w sprawie stworzenia planu wdrożenia w Polsce poszczególnych technologii oraz uzależnienie tak widzianej strategicznej decyzji od strategii dla całej grupy kapitałowej danego operatora. Często podejmowana jest poza granicami naszego kraju.

Pozostałe technologie IoT, jak LoRa lub SIGFOX, wymagają inwestycji prywatnych podmiotów w rozwój infrastruktury, a do takiej decyzji może skłonić wyłącznie portfolio długoterminowych i wolumenowych kontraktów. Tym samym jednymi z kluczowych uczestników rynku, stymulujących rozwój powinny stać się przedsiębiorstwa z udziałem Skarbu Państwa, szczególnie te o zasięgu ogólnokrajowym, których rolą jest realizacja projektów inwestycyjnych IoT.

Projekty takie powinny wspierać możliwość dywersyfikacji dostawców, aby nie doprowadzić do zjawiska monopolizacji dla dostawcy rozwiązania w nowej technologii, które zamiast stymulować innowacyjność i rozwój, konserwują rynek na lata. Jest to szczególnie ważne w branżach, w których przedsiębiorstwa publiczne posiadają dominujący udział w rynku.

Propozycje działań rządu

Kluczem do rozwoju IoT w Polsce jest otwartość standardów, rozumiana jako pełna jawność metod wymiany danych na wszystkich warstwach gwarantowana ustawowo. W modelu tym, każde wdrożenie IoT wymagałoby dostarczenia zarówno samego rozwiązania jak i kompletnej jawnej dokumentacji dla zamawiającego wraz z wymogiem dostępności dla innych podmiotów. Takie podejście da praktycznie nieograniczone możliwości integracji zarówno dla małych projektów lokalnych jak i ogólnokrajowych i będzie stymulatorem innowacyjności, łączenia heterogenicznych rozwiązań. Jawność przełoży się także na poziom bezpieczeństwa, który wzrasta w systemach o otwartym dostępie do protokołów, gdzie bezpieczeństwo bazuje na przyjętych metodach kryptograficznych a nie „tajności" protokołu.

Zalecenia dobrych praktyk prowadzenia projektów IoT wyeliminują błędy proceduralne w nadzorowaniu projektów innowacyjnych. Obecne procedury przetargowe skupiają się na szczegółach technicznych, zamiast na ocenie wyników i jakości działania rozwiązań docelowych. Model SLA, gdzie dostawca gwarantuje jakość zabezpieczoną karami umownymi, zapewnia kupującemu bezpieczeństwo inwestycji. Dostawca ze swojej strony ma większą dowolność w wyborze środków technicznych dla realizacji założonych celów.

W celu zapewnienia jakości oraz wsparcia projektów realizowanych przez samorządy należy wypracować zestaw dobrych praktyk wraz z ustandaryzowanym słownikiem pojęć w obszarze IoT. Polskie firmy, naukowcy i prawnicy wraz ze wsparciem Ministerstwa Cyfryzacji powinny w dalszym toku prac Grupy IoT przygotować i opublikować „Polski Leksykon pojęć IoT", który będzie wykorzystywany w przetargach i zakupach na bazie Prawa Zamówień Publicznych i komercyjnie. Będzie to realne przekazanie wiedzy i informacji do samorządów.

W zakresie urządzeń IoT w miejsce regulacji należy wprowadzić dobrze zdefiniowane procedury oceny pomiaru jakości i dopuszczenia do użytkowania. Możliwe jest wprowadzenie dobrowolnych certyfikatów jakości przez jednostki komercyjne na ogólnych, wspólnych dla wszystkich, warunkach np. przez operatorów telekomunikacyjnych, które zwiększałyby wiarygodność docelowych rozwiązań.

13

PRZEMYSŁ

W najbliższych latach przemysł stanie się jednym z sektorów, które w największym stopniu będą wykorzystywały technologie IoT. Rozwój polskiej gospodarki w dużej mierze zależy od innowacyjności i umiejętności wdrażania nowych rozwiązań. Pojawiające się bariery czy brak efektywnego wsparcia mogą wpłynąć na ograniczenie jej dynamicznego rozwoju.

AUTORZY:
KAMIL NAWROCKI, BCONNECT – LIDER PODGRUPY
SZYMON BONIECKI, MONTERAIL
DARIUSZ GOŁĘBIEWSKI, PZU LAB S.A.
DARIUSZ NACHYŁA, EVERY EUROPEAN DIGITAL
TOMASZ SERAFIN, AIUT SP Z O.O.
BOGDAN ŚLĘK, SIGNIFY POLAND SP. Z O.O.
JAROSŁAW WIDÓREK, COMARCH S.A.
TOMASZ ZALEWSKI, BIRD & BIRD KANCELARIA PRAWNA

Ogólna charakterystyka branży

Przemysł jest branżą, która od lat wykorzystuje technologię dla optymalizacji procesów wytwórczych i logistycznych. Specyfika operacyjna tych procesów (duże wolumeny, wysokie koszty przestojów i awarii, wysokie koszty i długie okresy amortyzacji parku maszynowego) sprawia, że jest to sektor silnie zorientowany na zagadnienia optymalizacji wydajności i ograniczania ryzyka operacyjnego. Jednocześnie sektor ten staje dziś przed nowymi wyzwaniami:

- skracanie cykli życia produktów,
- wahania popytu rodzące konieczność bardziej elastycznych cykli w procesach wytwórczych i logistycznych,
- trend przekształcania produktów w inteligentne usługi, sprawiający, że elementy koncepcji Internetu Rzeczy pojawiają się w architekturze produktów i wpływają na charakter procesów wytwórczych.

Powstawanie nowych kategorii produktów pozwala na budowę potencjału wytwórczego w pełni wykorzystującego potencjał nowych technologii (np. koncepcja „Giga Factory" firmy Tesla). W rezultacie światowe firmy produkcyjne i logistyczne podejmują dziś działania prowadzące do transformacji, których ramy zdefiniowane zostały w koncepcji Przemysł 4.0 (ang. *Industry 4.0*).

W Polsce obecne są średnie i duże firmy w szczególności z branży energetycznej i paliwowej, przemysłu ciężkiego, elektrotechnicznego, motoryzacyjnej, meblarskiej oraz innych branż. W różnym stopniu są one gotowe do inwestowania w nowe technologie, w automatyzację i kontrolę procesów produkcyjnych. Bariery dla modernizacji w duchu koncepcji „Przemysł 4.0" stanowią z jednej strony brak wiedzy, brak wzorców oraz niepewność co do rachunku ekonomicznego stojącego za inwestycjami związanymi z cyfrową transformacją przemysłu. Z drugiej jednak strony rośnie presja na podjęcie tych działań. Polskie przedsiębiorstwa będące kooperantami globalnych firm motoryzacyjnych widzą na przykład, że czeka je konieczność dostosowania do nowej klasy procesów i wymagań operacyjnych (czasy reakcji, elastyczność, jakość). Firmy, które z powodzeniem eksportują swoje produkty, często również zauważają konieczność dostosowania ich do realiów cyfrowego biznesu i cyfrowego stylu życia. W najtrudniejszej sytuacji są lokalne firmy średniej wielkości. Brak skali sprawia, że inwestycje w modernizację mają niską efektywność, a zwiększają dodatkowo niepewność podejmowania decyzji. Jednak i tutaj pojawia się presja (na przykład trudność z pozyskiwaniem pracowników) i możliwości (finansowanie unijne), które mogą prowadzić do rosnącego zainteresowania możliwościami Internetu Rzeczy, zwłaszcza w kontekście automatyzacji produkcji i intra-logistyki.

Po drugiej stronie rynku, dynamicznie rozwijają się firmy technologiczne działające w obszarze Industrial IoT (przemysłowe IoT – IIoT) i nowych technologii, które są gotowe na dopasowanie, rozwój i wdrożenie swoich najlepszych produktów we wszystkich gałęziach przemysłu, wszędzie tam, gdzie może to być oczekiwane lub przydatne. Warto wspomnieć o rozwoju polskich firm typu *Design House*, świadczących usługi projektowania i produkcji dedykowanej elektroniki, czy pojawiających się firm tworzących inteligentne systemy dla intra-logistyki opartych na autonomicznych robotach mobilnych (ang. *Self-Guided Vehicles*) własnej produkcji.

W Polsce znajduje się również wiele ośrodków naukowo-badawczych oraz uczelni wyższych realizujących badania z obszaru Industrial IoT, AI, rzeczywistości wirtualnej (VR) i rozszerzonej (AR), machine learning, Big Data, czy User Experience, które w aktywny sposób mogą wspierać rozwój IIoT.

Perspektywa rozwoju branży

Nowoczesny przemysł jest motorem rozwojowym gospodarki w ujęciu globalnym i lokalnym. Kraje pozbawione możliwości ekspansji są skazane na marginalizację na światowym rynku. Większość firm działających w branży jest otwarta na tworzenie nowych zakładów przemysłowych praktycznie niezależnie od granic państw. Tworzy to szereg możliwości migracji kapitału i technologii między gospodarkami. Kluczową szansą na przyciąganie inwestycji i rozwój istniejących, jest posiadanie stabilnych regulacji prawnych oraz odpowiedniej kadry, najlepiej posiadającej specyficzne kwalifikacje. Wciąż istotnym elementem jest koszt działalności w danym kraju – w tej dziedzinie Polska jest dalej atrakcyjna, jednak wiele wskazuje na to, iż poziom kosztów w krajach UE będzie się stopniowo wyrównywać, co jest zagrożeniem dla utrzymania wysokiego popytu na inwestycje i rozwój na terenie naszego państwa. Działalność operacyjna przedsiębiorstw jest silnie uzależniona od możliwości logistycznych – dostępności odpowiednich dróg, kolei, portów, lotnisk cargo i pasażerskich – przekłada się to na konieczność zaangażowania państw we właściwe planowanie rozwoju infrastruktury również pod kątem działalności przemysłowej, która często wymaga specyficznych rozwiązań (wysoka przepustowość, duży tonaż itp.). Inwestycje w infrastrukturę powinny również uwzględniać zapewnienie możliwości stabilnych dostaw energii (gwarancja dostępności właściwej mocy przyłączeniowej oraz niezawodności sieci przesyłowej) oraz istnienie odpowiednich sieci teleinformatycznych (wysoka przepustowość i niezawodność łączy radiowych i kablowych – światłowodowych). Przemysł napotyka na coraz większe bariery ze strony regulacji środowiskowych. Bardzo dużym wyzwaniem jest spełnianie kolejnych norm, które są istotne dla kondycji środowiska naturalnego, jednak często nie uwzględniają interesów branżowych.

Przemysł, w ujęciu ogólnym, jest jedną z najbardziej zaawansowanych technologicznie branż na świecie,

SYSTEM FUELPRIME – IOT W SIECI STACJI BENZYNOWYCH

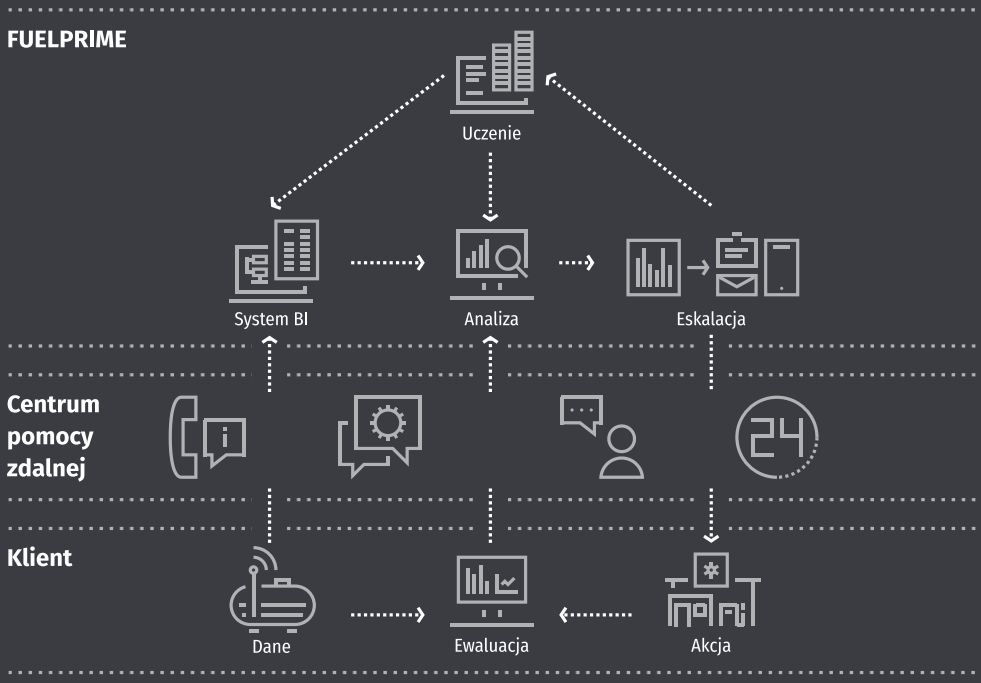
EUROPA / POLSKA

PROBLEM

Duże straty wynikające z nieoptymalnej organizacji procesu dystrybucji paliw z rafinerii do klienta końcowego.

ROZWIĄZANIE

System FuelPrime wdrożony w sieci stacji Shell na terenie Polski. System kontroluje paliwa płynne na każdym etapie dystrybucji, porównując różnice pojawiające się w procesach przelewania oraz monitoruje proces poboru paliw przez klientów z dystrybutorów na stacjach.



Każdy terminal paliwowy, cysterna i stacja paliw została wyposażona w dedykowane czujniki i koncentratory danych. Zbudowano też centralny system zarządzający oraz helpdesk. Firma AIUT świadczy kompleksową usługę – począwszy od produkcji urządzeń, poprzez instalację, do obsługi systemu 24/7. Wysoką skuteczność uzyskano dzięki dokładnym czujnikom zaprojektowanym specjalnie do pomiarów paliw oraz dzięki metodzie opartej na analizie dużych zbiorów danych tzw. Business Intelligence (BI). Serwer FuelPrime, umożliwia zarówno analizę bieżących danych jak też dostęp do danych historycznych oraz przesyła powiadomienia e-mail lub sms o sytuacjach krytycznych, do których zalicza się próby ingerencji w urządzenia lub pojawienie się nieprzewidywalnego wypływu paliwa. Czujniki FuelPrime są „wandalo oporne" oraz posiadają atesty do pracy w strefach zagrożenia wybuchem.

KORZYŚCI

- Pełna kontrola nad poziomem paliwa – system pozwala im przewidywać konieczność zamówienia dostawy
- Redukcja ryzyka operacyjnego – praktyczna eliminacja strat paliw płynnych (wdrożone w Shell rozwiązanie przyniosło redukcję strat do poziomu zaledwie 5l/24h w skali kraju).
- Zarządzanie dostawami (potwierdzenia, monitorowanie) – eliminacja niepotrzebnych transportów

od przynajmniej 60 lat poddawanej automatyzacji i robotyzacji. Obecnie jednak jest znacznie mniej podatny na innowacje, niż np. branża IT, gdzie działają światowi giganci produktów nowatorskich. Prowadzi to do trudności we wdrażaniu nowinek – szczególnie, gdy nowe metody, czy urządzenia są związane z bezpieczeństwem na terenie hal produkcyjnych lub pozwalają na uzyskanie zewnętrznego dostępu do danych o produkcji (np. otwarcie teleinformatycznych sieci przemysłowych na potrzeby IIoT). Dlatego bardzo istotne są działania propagatorskie, pokazujące korzyści wynikające z wdrażania rozwiązań innowacyjnych. Szczególną rolę w tego typu działalności powinien odegrać rząd w kooperacji z firmami (konferencje, wspólne prace nad standardami, publikacje naukowe i w prasie branżowej). Pojęcie *Industrial Internet of Things* istnieje w serwisie Wikipedia w języku angielskim dopiero od maja 2017 roku i od tego czasu miało jedynie 5000 wyświetleń, co wskazuje na konieczność propagowania terminu w branży.

Polskie firmy są coraz częściej obecne w świecie i poza utrzymywaniem własnych zakładów na terenie kraju, starają się otwierać filie nie tylko w państwach o gospodarkach rozwijających się, ale również w takich miejscach jak USA, czy Niemcy. Sprzyja to wymianie technologii i transferu wiedzy do tych organizacji również w obszarze IIoT.

Zakres możliwego wykorzystania IoT

Industrial IoT należy na początku podzielić na dwa typy:

- Offline IIoT – rozwiązania, które wspierają zbieranie odpowiednio dużej ilości danych i pozwalają na ich późniejszą obróbkę, celem optymalizacji procesów – nie mają wpływu na bieżącą operacyjność zakładów przemysłowych, dopóki efekty analizy danych nie pozwolą na wprowadzenie zmian,

- Online IIoT – narzędzia i systemy, które działają operacyjnie i wpływają na bieżąco na proces pracy zakładu przemysłowego.

W wielu przypadkach wdrożenie systemu IIoT pozwala na uzyskanie narzędzia zarówno online i offline, a często następuje przenikanie się tych funkcji. Należy jednak zaznaczyć, że dostęp do danych offline może być utrudniony w wielu sytuacjach ze względu na ryzyko gromadzenia danych przemysłowych oraz konieczność inwestycji w moce obliczeniowe i odpowiednie oprogramowanie do analiz dużych zbiorów danych.

Podstawowym zadaniem systemów IIoT jest optymalizacja procesów przemysłowych – począwszy od efektywności pracy a skończywszy na zużyciu zasobów surowcowych. W efekcie wszystko zbiega się do redukcji ryzyka i kosztów działalności.

Pierwszym istotnym elementem jest łańcuch logistyczny. Posiadanie informacji o dokładnym czasie dostaw towarów niezbędnych do produkcji oraz o potencjalnych opóźnieniach, pozwala niemalże natychmiastowo reagować i w razie problemów np. przezbrajać linie produkcyjne. Takie możliwości dają systemy lokalizacji pojazdów spięte z centralnym systemem zarządzania produkcją (np. kierowcy ciężarówek mogą zgłaszać awarie, opóźnienia, bezpośrednio ze swojego pojazdu „w czasie rzeczywistym").

Jeżeli dany zakład przemysłowy ma już dostarczone komponenty, trzeba je odpowiednio magazynować i dystrybuować wewnątrz. Do tego celu można budować systemy informujące o zajętości regałów oraz prowadzić ruch autonomicznych pociągów logistycznych (wózków), które odbiorą materiał z właściwego miejsca i dostarczą na daną linię – w rygorze czasu i uwzględniając optymalną ścieżkę przejazdu po terenie hali produkcyjnej. Posiadanie informacji historycznej o zajętości regałów pozwala wykonywać analizy offline i decydować o konieczności rozbudowy lub redukcji przestrzeni magazynowej w zależności od prowadzonej w danym czasie działalności.

Każda paczka, każdy pojazd autonomiczny, czy sterowany przez człowieka oraz wszyscy pracownicy powinni być lokalizowani na terenie zakładu. Do tego celu służą systemy IIoT do lokalizacji wewnątrz budynków. Umożliwiają bieżące śledzenie każdego ruchomego obiektu w fabryce. Operatorom ruchu dają podgląd sytuacji w zakładzie i pozwalają reagować w sytuacjach krytycznych. Analiza danych offline z systemu lokalizacji umożliwia optymalizację zatrudnienia, pozwala modyfikować ścieżki przejazdowe w halach itp.

Aby jeszcze bardziej usprawnić funkcjonowanie zakładów, należy kontrolować parametry środowiskowe – takie jak temperatura, wilgotność, poziom zapylenia, co pozwala np. odpowiednio zarządzać przerwami pracowników, czy serwisowaniem maszyn, jak również wyprzedzać awarie urządzeń (ang. *predictive maintenance*) – jeżeli nadzorca zobaczy np. wzrost wilgotności w danym obszarze hali, może wysłać na miejsce serwisanta, który wyłączy maszynę, zmieni parametry jej pracy lub wykryje awarię innego urządzenia, które może wpłynąć na operacyjność (np. awarię wodociągu).

Kontrola wszelkich parametrów środowiskowych jest również powiązana z zagadnieniami inteligentnych budynków – zarządzanie zużyciem energii w zakładach jest kluczowe dla redukcji kosztów – najprostszym przykładem IIoT w tej dziedzinie jest inteligentne oświetlenie bazujące na czujnikach zmierzchu oraz ruchu.

Gromadząc dane z dowolnego systemu IIoT działającego online, można prowadzić szereg analiz offline, które mogą doprowadzić do powstania kolejnych oszczędności i optymalizacji – np. analizując ruch pracowników na terenie hali, można zaplanować redukcję urządzeń oświetleniowych lub mało uczęszczane ścieżki przeznaczyć na przestrzeń magazynową (uwzględniając reguły BHP, co też może być brane pod uwagę przez modele matematyczne).

Nowoczesne firmy produkcyjne, które chcą wdrożyć koncepcje Industry 4.0, sięgają najczęściej właśnie po IIoT przede wszystkim w celu uzyskania dokładnej analizy danych z urządzeń, które komunikują się ze sobą w czasie rzeczywistym (Online IIoT). Zasoby firmy, wytwarzane towary, dane, rynek i klienci stanowią ekosystem, który wymaga wydajnych środków dostępu i wymiany informacji.

W przedstawionym poniżej przypadku mówimy o stworzeniu ekosystemu IIoT dla rozwiązań, które charakteryzują się szerokim zakresem możliwości rozwoju (skalowania) zarówno sprzętowego, jak i programowego. Głównym składnikiem tego ekosystemu może być platforma IIoT. Łącząc platformę IIoT dzięki komponentom sieciowym, takim jak koncentratory IoT (przekaźniki), sygnalizatory i znaczniki RFID (nadajniki), możliwe jest zapewnienie komunikacji w czasie rzeczywistym i zbieranie danych z maszyn oraz czujników. W ten sposób zapewniana jest kontrola i ciągłość dostępu do danych w całym łańcuchu produkcyjnym, od komunikacji między urządzeniami poprzez linię montażową, aż po procesy zarządzania i dystrybucję produktów do klienta.

Źródło: Comarch SA

Jednym z najbardziej spektakularnych i przyszłościowych systemów IIoT jest tzw. VR lub AR. VR umożliwia wirtualne szkolenia pracowników na bazie wizualizacji maszyn lub całych zakładów z wirtualnymi asystentami. AR to natomiast narzędzie np. dla serwisantów, którzy chodząc po zakładzie produkcyjnym w okularach z wbudowanym wyświetlaczem, podchodząc do maszyny, dostają pełną informację diagnostyczną i w wypadku awarii wirtualną instrukcję naprawy.

Branża IIoT tworzy nowe możliwości dla przemysłu – proces produkcyjny urządzeń IIoT często bazuje na rozwiązaniach innowacyjnych, dzięki czemu doświadczenia zdobyte w jego trakcie, mogą służyć za wzór dla zakładów przemysłowych pracujących w innych sektorach rynku.

Bariery

Bariery należy podzielić na dwie kategorie:

- wewnętrzne – powiązane z procedurami w zakładach produkcyjnych,
- zewnętrzne – związane z rozwojem rynku IIoT.

Bariery wewnętrzne związane są z wysoką regulacją każdego zakładu przemysłowego. W warunkach rynku polskiego, większość zakładów przemysłowych należy do firm z kapitałem zagranicznym, co powoduje, iż bardzo często są importowane procedury korporacyjne i globalne. Tutaj należy się wykazać wysoką skutecznością we wdrażaniu innowacji, co może dawać szanse na ekspansje na globalne rynki (lokalny

OPTYMALIZACJA PROCESU PRODUKCJI DZIĘKI IoT

SZWAJCARIA

PROBLEM

W szwajcarskiej firmie ABNOX produkowano krótkie serie produktów w oparciu o montaż ręczny, co generowało bardzo duże straty i wysokie koszty ich wytworzenia. Niedostateczna kontrola procesu produkcyjnego oraz drukowanie papierowych wytycznych dla pracowników rodziły spore problemy zarządcze i uniemożliwiały właściwy proces nadzoru jakości. Klient nie rozważał zakupu nowego sprzętu, dlatego konieczne było przeprowadzenie retrofittingu i wykorzystanie obecnej infrastruktury.

ROZWIĄZANIE

W firmie ABNOX eksperci Comarch wdrożyli rozwiązania IoT z zakresu Industry 4.0. integrując proces produkcji z systemem Comarch ERP, równocześnie wyposażając linię produkcyjną (i jej poszczególne elementy) w detektory rejestrujące status, kolejność i czas każdego z etapów. Dodaliśmy do niej specjalne ekrany, dzięki którym pracownicy są informowani o kolejności wykonywanych zadań i szczegółowych instruktażach montażowych (tym samym zrezygnowaliśmy z papierowych dokumentów produkcyjnych). Dodatkowo u klienta wdrożyliśmy Zintegrowany System Realizacji Produkcji (MES), który umożliwia zbieranie i analizę danych w czasie rzeczywistym, zapewniając pełną kontrolę nad procesem wytwórczym.

KORZYŚĆ

Dzięki zastosowanym rozwiązaniom Comarch IoT klient zautomatyzował część prac linii produkcyjnej (m.in. proces obsługi znakowarki laserowej), skrócił czas produkcji, umożliwiając zwiększenie liczby produkowanych wariantów swoich urządzeń do ponad 100, diametralnie zmniejszając liczbę błędów pracowniczych oraz krzywą uczenia się nowych pracowników. Zredukował pracę produkcji o 50%, a wdrożone przez Comarch rozwiązanie pozwoliło mu skutecznie kontrolować wszystkie etapy procesu produkcyjnego, eliminując koszt zakupu nowego sprzętu i unowocześniając starszy system niższym kosztem. Obecnie zbierane przez niego dane produkcyjne służą analizie biznesowej i są wykorzystywane do dalszych procesów optymalizacyjnych.

zakład może przekazać technologię placówkom w innych krajach).

Bariery zewnętrzne są problemem rozwojowym powiązanym z możliwością pozyskania odpowiedniego wykonawcy systemu IIoT. Wiele firm dysponuje np. oprogramowaniem do obsługi IIoT, ma jednak problem z dostarczeniem odpowiedniego wolumenu urządzeń fizycznych i dostosowaniem ich do często trudnych warunków przemysłowych. W warunkach polskich istotne byłoby wspieranie lokalnych producentów, którzy są w stanie zapewnić dostawy na rynek polski i dać szansę na ekspansję globalną np. na rynku specjalizowanych czujników, czy systemów lokalizacyjnych wewnątrz hal przemysłowych.

W celu rozwoju IIoT należy również stymulować sektor publiczny. Firmy z tego sektora powinny otworzyć się na wdrożenia IIoT np. w wyniku deregulacji zamówień na systemy innowacyjne. Dotyczy to zwłaszcza sektorów podlegających przepisom prawa zamówień publicznych takich jak górnictwo, porty lotnicze i morskie, energetyka, transport kolejowy. Wdrożenia IIoT ze względu na ich nowatorstwo wymagają wkomponowania w proces udzielania zamówienia publicznego elementów promujących innowacyjność. Niestety obecna praktyka w Polsce nie promuje tego typu postępowania. W Polsce od dawna mówi się o tym, że zamówienia publiczne winny promować innowacyjność. W kwietniu 2008 roku Rada Ministrów przyjęła dokument „Nowe podejście do zamówień publicznych. Zamówienia publiczne a małe i średnie przedsiębiorstwa, innowacje i zrównoważony rozwój". Powstało także szereg opracowań, raportów i badań wskazujących na potrzebę proinnowacyjnego podejścia do zamówień publicznych. Jednak te wszystkie

działania nie doprowadziły do istotnej zmiany w tym zakresie. Z pewnością jednym z powodów było to, że wspieranie innowacyjności było w hierarchii ważności problemów polskich zamówień publicznych na dość odległym miejscu. Polski system zamówień publicznych przez ostatnie lata zmagał się z innymi kwestiami o fundamentalnym charakterze, jak chociażby zmiana podejścia do kryteriów oceny ofert i odejście od stosowania wyłącznie kryterium ceny. Nie pomagał też formalizm postępowania i restrykcyjne podejście kontrolujących do wszelkich niestandardowych rozwiązań stosowanych przez zamawiających. Są oczywiście przykłady polskich innowacyjnych zamówień publicznych, jednak mają one charakter wyjątku od reguły.

Propozycje działań rządu

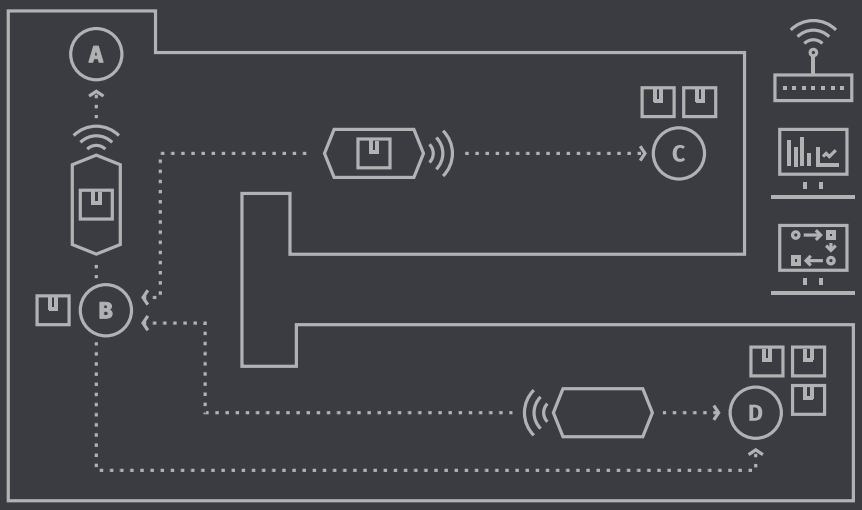
Rekomendujemy następujące działania:

- Opracowanie Narodowej Strategii Rozwoju IoT dla Przemysłu.
- Podniesienie skuteczności wykorzystania funduszy unijnych na projekty B+R.
- Zwiększenie zaangażowania sektora publicznego w inwestycje wysokiego ryzyka, jakim jest obszar nowych technologii, poprzez np. ułatwienie przeprowadzenia pilotaży rozwiązań.
- Stałe wspieranie rozwoju małych i średnich spółek technologicznych, w tym start-up'ów, np. poprzez dedykowane programy PFR.
- Realne wsparcie dla MŚP umożliwiające faktyczny transfer wiedzy z nauki do biznesu za pośrednictwem spółek technologicznych oraz wymianę informacji i zapotrzebowania, dzięki którym możliwe byłoby wypracowanie strategicznych projektów z obszaru IIoT.
- Wypracowanie mechanizmów, jasnych i jednoznacznych standardów, a także zweryfikowanych i zaakceptowanych wzorców dokumentów postępowań dotyczących zamówień publicznych i zakupów innowacyjnych technologii.
- Aktywne promowanie innowacyjnych zamawiających i odpowiednie ukształtowanie wytycznych dotyczących kontroli innowacyjnych zamówień tak, aby formalistyczne mechanizmy kontrolne nie powodowały niechęci zamawiających do zakupu innowacyjnych rozwiązań IIoT.
- Wyposażenie zamawiających w narzędzia w postaci opisów dobrych praktyk udzielania innowacyjnych zamówień publicznych oraz zamówień przedkomercyjnych. Zamówienia przedkomercyjne są to zamówienia na prace badawczo-rozwojowe współfinansowane przez wykonawców, które mają perspektywę komercjalizacji i objęcia ich potem zamówieniami publicznymi. Poprzez przedkomercyjne zamówienia publiczne sektor publiczny mógłby istotnie wesprzeć polski przemysł rozwijający rozwiązania IIoT i dać mu szansę rozwinięcia innowacyjnych produktów, które potem mogłyby zostać zaoferowane zarówno na rynku krajowym jak i na rynku światowym.
- Współpraca wszystkich Interesariuszy (przemysł, spółki technologiczne, jednostki naukowo-badawcze i uczelnie) w ramach Fundacji Platforma Przemysłu Przyszłości w kontekście Strategii na rzecz Odpowiedzialnego Rozwoju. Pierwszym i najpilniejszym celem niedawno powołanej do życia Fundacji Platformy Przemysłu powinna być popularyzacja tematu Przemysłu 4.0 poprzez budowanie świadomości o potrzebie transformacji cyfrowej oraz transfer doświadczeń i wiedzy do potencjalnych partnerów. W celu zapewnienia pełnej efektywności działań Fundacji niezbędne jest aktywne zaangażowanie jak najliczniejszych środowisk, w szczególności biznesowych, w inicjatywy Fundacji. Tym bardziej, że do tej pory to zainteresowanie było dość umiarkowane, o czym świadczy chociażby niewielki udział w publicznych konsultacjach projektu ustawy dotyczącej Platformy (na 85 zaproszonych podmiotów, wzięło udział jedynie 8). Jako przykład może posłużyć niemiecka „Platforma Przemysłu 4.0", która łączy działania różnych środowisk związanych z przemysłem porządkuje różne formy zastosowań rozwiązań technologicznych w przemyśle w ramach scenariuszy wdrożeń, tworzy wspólne ramy referencyjne oraz przygotowuje opracowania na tematy związane z rozwojem Przemysłu 4.0. Platforma zachęca do podjęcia współpracy, informując na stronie internetowej o możliwości włączenia się w prace poszczególnych grup i podgrup roboczych, czy o możliwości podzielenia się doświadczeniami z wdrożeń z innymi przedsiębiorcami poprzez wysłanie informacji w celu publikacji na mapie wdrożeń[1].

1 https://www.plattform-i40.de/I40/Navigation/Karte/SiteGlobals/Forms/Formulare/karte-anwendungsbeispiele-formular.html

ROBOTYZACJA INTRA-LOGISTYKI AUTONOMY@WORK

POLSKA



PROBLEM

Procesy intralogistyczne (zapewniające przepływ materiałów i komponentów pomiędzy gniazdami produkcyjnymi, magazynami I buforami logistycznymi) stanowią istotny składnik procesów wytwórczych. O ile robotyzacja czynności związanych z wytwarzaniem ma w przemyśle długą tradycję, to procesy intralogistyczne nadal realizowane są przez prostą automatyzacje – podajniki taśmowe, wózki widłowe i urządzenia transportowe wymagające obsługi operatora. Istniejące rozwiązania nie nadążają za potrzebami Przemysłu 4.0, wymagającymi zwiększania elastyczności linii produkcyjnych w związku ze zmiennością cykli, asortymentów czy konfiguracji. Problemem są też wypadki z udziałem pracowników, które generują koszty związane ze wstrzymaniem produkcji, dochodzeniami wyjaśniającymi i procesami odszkodowawczymi.

ROZWIĄZANIE

Systemy intralogistyczne, oparte o autonomiczne roboty mobilne (AGV / SGV) – urządzenia zdolne do samodzielnej nawigacji w dynamicznym środowisku współczesnej fabryki dostosowane do typowych zadań transportowych i zintegrowane z systemami zarządzania produkcją. Rozwiązanie takie proponuje m.in. polska spółka VersaBox. Platforma intralogistyczna VersaBox wykorzystuje zaprojektowane i produkowane przez firmę roboty mobilne, posiadające certyfikację w zakresie wymaganych norm bezpieczeństwa. Pilotażowe wdrożenia weryfikujące ich przydatność w warunkach rzeczywistego systemu produkcji miały miejsce w fabrykach dostarczających komponenty dla przemysłu samochodowego i są dzisiaj wdrażane produkcyjnie w kolejnych zakładach. System nawigacyjny TRUE AUTONOMY® rozwijany przez specjalistów VersaBox jest też wykorzystywany do „autonomizacji" wyspecjalizowanych urządzeń firm trzecich.

https://versabox.eu/smart-intra-logistics/

KORZYŚĆ

Zmniejszenie wypadkowości, usprawnienie obsługi linii produkcyjnej i w efekcie obniżenie kosztów produkcji.

14

ROLNICTWO I OCHRONA ŚRODOWISKA

Zastosowanie Internetu Rzeczy w rolnictwie i ochronie środowiska może pomóc w rozwiązywaniu istotnych problemów cywilizacyjnych, takich jak optymalizacja produkcji oraz podniesienie jakości żywności, monitoring zmian i zjawisk w środowisku naturalnym (np. smog, susza, zanieczyszczenie wód) oraz wsparcie w podejmowaniu adekwatnych działań.

AUTORZY:
MARCIN PŁÓCIENNIK, ICHB PAN, POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO SIECIOWE (PCSS) – LIDER PODGRUPY
JERZY BIAŁOUSZ, INVENTIA SP. Z O.O.
RAFAŁ MAŃKOWSKI, POLSKA IZBA UBEZPIECZEŃ
MICHAŁ MISIEK, AIRLY SP. Z O.O.
TOMASZ RAJTAR, ICHB PAN, PCSS

Ogólna charakterystyka branży

Rolnictwo zwiększa wydajność swojej produkcji przez zastosowanie nowoczesnych technologii ICT do gromadzenia, przetwarzania i analizy danych, jak również do automatyzacji procesów w celu optymalizacji działania gospodarstw.

Według danych GUS w Polsce mamy około 1,4 mln gospodarstw rolnych. Dominują przede wszystkim gospodarstwa małe i średnie. Zaledwie 20% ogółu powierzchni rolnych stanowią gospodarstwa ponad 20 ha. Łączna powierzchnia użytków rolnych wynosi około 18810,1 tys. ha, a gruntów leśnych i zadrzewionych ok. 9513,2 tys. ha.

Wyzwania w rolnictwie w Polsce to: obniżenie kosztów produkcji, zapotrzebowania na pracę ręczną, optymalizacja wykorzystania wody, nawozów, pestycydów, zwiększenie bezpieczeństwa produkcji i dostaw żywności, stosowanie praktyk rolniczych zgodnych z ochroną środowiska naturalnego (różnorodności biologicznej, wody, gleby) i monitorowanie cyklu produkcyjnego.

Najważniejszą presję na modernizację produkcji żywności w Polsce wytwarzają dzisiaj duzi dystrybutorzy (np. duże sieci sklepów) narzucający z jednej strony rygorystyczny monitoring jakości produktów, co jest między innymi pochodną regulacji unijnych tej branży, z drugiej zaś zmuszający producentów do efektywności poprzez swoją siłę przetargową. To sprawia, że rolnictwo staje się dzisiaj branżą, która zaczyna przyciągać innowatorów podejmujących udane eksperymenty z wykorzystaniem rozwiązań IoT wspierających efektywną ekonomicznie i zapewniającą właściwą jakość produkcję. Jednym z istotnych warunków „uprzemysłowienia" tych eksperymentów wydaje się być postęp w konsolidacji producentów, czy to poprzez mechanizmy spółdzielcze czy kapitałowe.

Ochrona środowiska to branża skupiająca się na dążeniu do redukcji i naprawy szkód wyrządzonych otoczeniu fizycznemu lub zasobom naturalnym. Ochrona środowiska napotyka szereg wyzwań, którymi są między innymi wzrost temperatury Ziemi, zanieczyszczenia powietrza, gospodarka odpadami, skażenie środowiska substancjami toksycznymi, nagromadzenie odpadów zagrażających środowisku naturalnemu, pożary, ochrona bioróżnorodności gatunkowej i lasów, ochrona wód śródlądowych i morskich.

Znajdujące się wysoko na liście zagrożeń globalne ocieplenie napędzane jest w dużej mierze przez tzw. gazy cieplarniane, m.in. dwutlenek węgla, metan, parę wodną. Istotne jest monitorowanie ich stężenia oraz źródeł emisji – pozwala ono oszacować wpływ i podejmować działania wpływające na redukcję emisji.

Wszechobecność pojazdów spalinowych, tzw. niska emisja, emisja z przemysłu, pożary lasów mają z kolei bezpośredni wpływ na jakość powietrza. Zanieczyszczenie powietrza jest jednym z ważniejszych problemów, z którym starają sobie poradzić kraje europejskie. W 2016 roku zanieczyszczenie powietrza było według szacunków przyczyną śmierci 4,2 miliona ludzi na całym świecie. Niestety, jesteśmy liderem w kategorii zanieczyszczenia powietrza: 36 z 50 najbardziej zanieczyszczonych miast europejskich znajduje się w Polsce. Roczne normy europejskie odnośnie limitów stężenia pyłów zawieszonych PM2,5 i PM10 są u nas wielokrotnie przekraczane. Główną przyczyną jest niska emisja – ogrzewanie domów w oparciu o niewydajne piece węglowe oraz paliwo niskiej jakości generujące duże ilości pyłu zawieszonego. Problemem jest również koncentracja benzo-a-pirenu, którego zmierzone stężenia w okresie zimowym na terenie Polski przekraczały dopuszczalną normę 1 ng/m^3 kilkanaście razy.

Najważniejsze wyzwania w temacie ochrony środowiska w Polsce to: poprawa jakości powietrza, lokalizacja głównych źródeł zanieczyszczenia pyłami, gazami toksycznymi i lotnymi związkami organicznymi (ang. *VOC*, np. benzo(a)piren), neutralizacja zagrożenia ze strony susz i zanieczyszczenia wód, ograniczenie erozji gleby oraz eutrofizacji wód, podniesienie efektywności nawadniania roślin, mitygacja zagrożeń dla zwierząt i roślin (agrofagi, zmniejszanie populacji gatunków i bioróżnorodności).

Perspektywa rozwoju branży

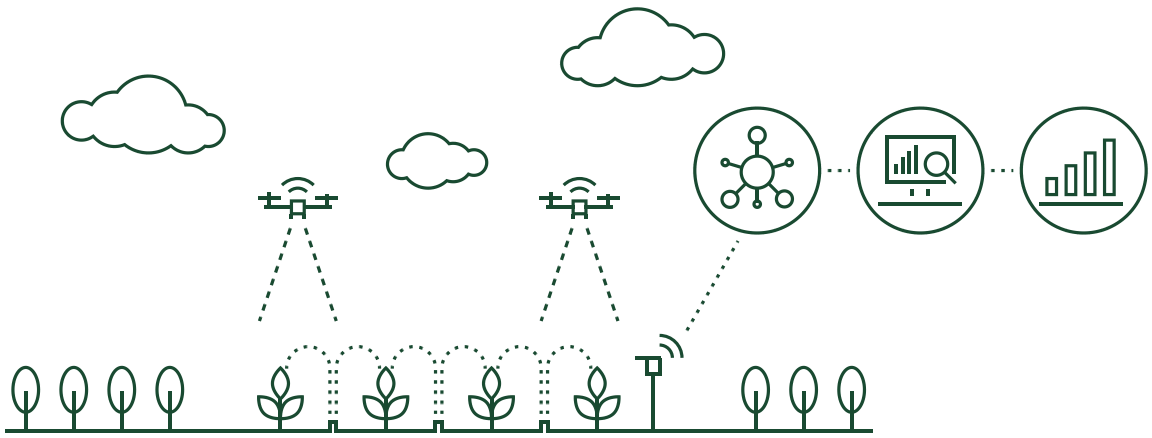
Rolnictwo w Polsce i na świecie staje przed dużymi wyzwaniami cywilizacyjnymi, związanymi ze wzrostem populacji do 9 mld ludzi około 2050 roku i idącym za nim wzrostem zapotrzebowania na żywność. Niezbędna jest optymalizacja produkcji żywności, zwiększająca wydajność o około 70 procent. Internet Rzeczy jest w tym świetle jedną z kluczowych technologii, która ma duży potencjał w zakresie wsparcia zarządzania i optymalizacji procesów w rolnictwie.

Pokrewne wyzwania cywilizacyjne są też związane z ochroną środowiska (problemy smogu, suszy, zanieczyszczenia wód, erozji gleb, wzrostu ich zasolenia, negatywne zmiany w środowisku naturalnym zwierząt i roślin). Internet Rzeczy jest kluczową technologią umożliwiającą monitorowanie tych zjawisk i wspierającą szybkie podejmowanie adekwatnych działań.

Rolnictwo

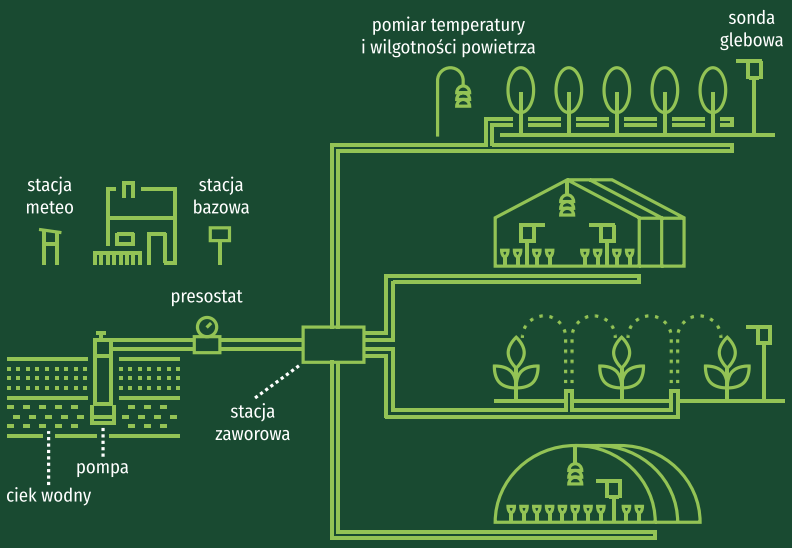
Potencjał działań w rolnictwie, obejmuje wiele aspektów między innymi:

- zwiększenie produktywności roślin poprzez zastosowanie precyzyjnej agrotechniki i ochrony roślin, intensyfikacja działań skierowanych na hodowlę bardziej plennych odmian, rozwój produkcji żywności funkcjonalnej, uwzględnienie w programach hodowlanych odporności roślin na stresy biotyczne (biologiczne, takie jak np. choroby i szkodniki roślin uprawnych) oraz abiotyczne (fizyczne, takie jak np. ekstremalne temperatury, ograniczona dostępność lub nadmiar wody, erozja gleby, silne wiatry),
- zwiększona rentowność rolnictwa wywołana zwiększonym popytem na dobre jakościowo i zdrowotnie produkty, ograniczenie oddziaływania na środowisko poprzez wdrożenie i rozwijanie integrowanej produkcji oraz rozwój rolnictwa ekologicznego,
- dalszy rozwój technologii przechowywania i przetwórstwa płodów rolnych, ograniczenie pracy ręcznej poprzez doskonalenie techniki zbioru,
- wprowadzenie robotyki do zbioru i pielęgnacji warzyw i owoców uprawianych pod osłonami (pomidor, ogórek, papryka, oberżyna, truskawki itp.), wprowadzenie autonomicznych maszyn do prac polowych i prowadzenia ochrony roślin,
- zwiększenie bezpieczeństwa pracy,
- rozwój systemów DSS (Decision Support System – systemy wspierania decyzji) pomocnych przy podejmowaniu kluczowych decyzji podczas uprawy ochrony i zbioru roślin.



PROJEKT eSAD

HTTPS://WWW.INVENTIA.PL/NEWSY/AGREUS-ROLNICTWO-4-0-CZYLI-IIOT-W-PRAKTYCE-ROLNEJ/
POLSKA



PROBLEM

Obecnie zaledwie kilkanaście procent z ankietowanych gospodarstw stosuje jakiekolwiek metody oceniania potrzeb wodnych plantacji. Brak systemów pozwalających na optymalizację nawadniania upraw ma bezpośredni wpływ na konkurencyjność polskich gospodarstw na tle przedsiębiorstw produkcji rolnej z krajów rozwiniętych technologicznie.

ROZWIĄZANIE

W Polsce w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego prowadzony jest projekt eSad – „Opracowanie innowacyjnego system pomiaru rozproszonego parametrów klimatyczno-glebowych jako narzędzia optymalizacji nawadniania, ochrony roślin i prac agrotechnicznych". W ramach projektu powstaje system Agreus.

KORZYŚĆ

System Agreus, wdrażany przez polską firmę Inventia, pozwala na daleko idące oszczędności w zużyciu wody w uprawie roślin przy użyciu sieci czujników pomiarowych (monitoring warunków klimatycznych i wilgotności gleby) oraz automatycznej stacji zaworowej.

KOMPLEKSOWY SYSTEM MONITORINGU POWIETRZA

HTTPS://AIRLY.EU/PL/COMPANY/
POLSKA

PROBLEM

Według corocznych raportów Europejskiej Agencji Środowiska (EEA) Polacy oddychają powietrzem bardzo złej jakości, przez co przedwcześnie umiera ponad 48 tysięcy osób. Pierwszym krokiem do poprawy sytuacji jest zwiększenie świadomości obywateli, a także umożliwienie lokalizacji źródeł problemu i najbardziej newralgicznych miejsc. Wysokie koszty instalacji i eksploatacji urządzeń monitorujących poziom zanieczyszczenia powietrza.

ROZWIĄZANIE

Kompleksowy system monitoringu jakości powietrza Airly stanowiący uzupełnienie stacji Państwowego Monitoringu Środowiska. Urządzenia posiadają wbudowany laser, który mierzy zawarte w powietrzu frakcje pyłu zawieszonego: PM1, PM2.5, PM10 oraz gazy toksyczne: dwutlenek azotu, ozon, dwutlenek siarki i tlenek węgla. System pozwala na analizę przestrzenną i dynamiczną stanu jakości powietrza w miastach, na terenach zabudowanych i obszarach wiejskich.

KORZYŚĆ

Zmniejszenie rozmiaru czujników smogu obniżyło koszty ich produkcji oraz utrzymania, w stosunku do stacji referencyjnych. Urządzenia charakteryzują się wysoką dokładnością pomiarów, która była wielokrotnie testowana w badaniach porównawczych, przeprowadzanych przez jednostki naukowe. Ze względu na znacząco niższe koszty, pozwalają oszacować stan jakości powietrza w miejscach, które nie były dotąd objęte systemami pomiarowymi. System Airly składa się z wielu elementów, które pozwalają m.in. informować mieszkańców o jakości powietrza poprzez platformę Web (https://airly.eu/map), aplikacje mobilne (iOS, Android), dostęp do danych poprzez interfejs programistyczny API, czy tablice informacyjne LED. Dodatkowo Airly dostarcza 24-godzinną prognozę jakości powietrza z wykorzystaniem sztucznej inteligencji (AI).

W Polsce główne działania prowadzone są w ramach europejskich funduszy strukturalnych m.in. PROW. Branża IoT ma potencjalnie możliwości zaangażowania się w większości priorytetowych działań wyznaczonych przez UE dla rozwoju obszarów wiejskich, min.:

- poprawa rentowności i konkurencyjności wszystkich rodzajów rolnictwa oraz promowanie innowacyjnych technologii dla gospodarstw rolnych i zrównoważonej gospodarki leśnej,
- poprawa organizacji łańcucha żywnościowego, dobrostanu zwierząt i zarządzania ryzykiem w rolnictwie,
- odtwarzanie, chronienie i wzmacnianie ekosystemów zależnych od rolnictwa,
- promowanie efektywnego gospodarowania zasobami i wspieranie przejścia na gospodarkę niskoemisyjną i odporną na zmianę klimatu w rolnictwie, sektorze spożywczym i leśnictwie.

Ochrona środowiska

Potencjał działań wiąże się z licznymi zagrożeniami dla środowiska i wyzwaniami wspomnianymi w poprzedniej sekcji. Technologie IoT oferują możliwość znacznej poprawy

w dziedzinie monitoringu środowiska przez zwiększenie liczby stacji pomiarowych – zarówno w postaci stacji referencyjnych, jaki i przez utworzenie monitoringu uzupełniającego o większej gęstości. Monitoring pozwala na tworzenie map zanieczyszczenia czy występowania negatywnych zjawisk, analizowaniu wpływu na środowisko (zastosowanie technologii Big Data, AI), zarządzaniu problemami i skutkami niekorzystnych warunków oraz podejmowania działań prewencyjnych. Dobrze zorganizowany monitoring daje skwantyfikowaną wiedzę o konkretnych parametrach środowiska czy procesu, pozwala na szybkie i skuteczne podejmowanie decyzji poprawiających sytuację w danej dziedzinie, pobór energii rozwiązań IoT, a tym samym efektywniejsze niż dotąd wykorzystanie bateryjnych źródeł energii.

Ponadto infrastruktura oparta na dedykowanych rozwiązaniach telekomunikacyjnych dla potrzeb opomiarowania (SigFox, LoRa) może być wykorzystywana w szerszym zakresie jako platforma komunikacji masowej urządzeń IoT, alternatywna do obecnie dostępnych (GSM, LTE).

Zakres możliwego wykorzystania IoT

Rolnictwo

- Zarządzanie używaniem nawozów i środków ochrony roślin.
- Zarządzanie zużyciem wody w produkcji rolnej / precyzyjne nawadnianie.
- Optymalizacja nawożenia / precyzyjne nawożenie.
- Monitoring szkodników i chwastów zagrażających uprawom, warunków środowiskowych – zastosowanie sensorów w uprawie i hodowli i ochronie roślin, hodowli zwierząt, nadzór nad fazami wzrostu.
- Precyzyjne karmienie.
- Śledzenie stanów magazynowych.
- Gospodarka odpadami i recykling w produkcji rolnej.
- Zarządzanie i monitoring gospodarki pasiecznej.
- Sterowanie klimatem w produkcji ogrodniczej pod osłonami jak również parametrami technologicznymi w chłodniach, przechowalniach i suszarniach.

Bezpieczeństwo żywności

- Monitoring łańcucha dostaw żywności (rolnik, przetwórca żywności, logistyka i magazynowanie, sprzedawca detaliczny, konsument – łączenie odpowiednich danych generowanych na każdym z etapów).

Ochrona środowiska

- Monitorowanie jakości powietrza z uwzględnieniem pyłów zawieszonych, gazów toksycznych (np. NO2, O3, CO) oraz lotnych związków organicznych (LZO, ang. *VOC*), dwutlenku węgla i potencjalnych miejsc jego emisji.
- Monitorowanie natężenia promieniowania jonizującego.
- Monitoring ciągły potencjalnych źródeł zanieczyszczenia powietrza, np. fabryk i zakładów produkcyjnych,.
- Monitoring jakości i ilości wód oraz występowania zakwitu glonów.
- Monitorowanie jakości gleby i podłoży ogrodniczych.
- Monitorowanie hałasu w środowisku naturalnym oraz na obszarach zurbanizowanych.

- Monitorowanie bioróżnorodności, stanu siedlisk.

- Monitoring w gospodarce odpadów.

Bariery

W toku prac, podgrupa zidentyfikowała następujące bariery:

- Brak pokrycia otwartymi sieciami bezprzewodowymi typu LPWAN.

- Brak edukacji w zakresie możliwości i rozwiązań IoT w rolnictwie, dających realne korzyści.

- Brak farm demonstracyjnych, które mogą być przykładem rozwiązań w zakresie zastosowania Internetu Rzeczy.

Propozycje działań rządu

Proponujemy następujące działania, mające na celu rozwój IoT w branży:

- Wsparcie dla działań mających na celu pokrycie całego obszaru kraju zasięgiem sieci łączności bezprzewodowej w technologii odpowiedniej dla urządzeń IoT z zasilaniem bateryjnym (np. LoRaWAN, Weightless , Sigfox, NB-IoT). W przypadku zastosowań w rolnictwie i ochronie środowiska (tereny słabo zaludnione z małą ilością stacji bazowych) potrzebna jest infrastruktura umożliwiająca przyłączenie wystarczającej ilości urządzeń – w tym również sensorów pracujących miesiącami czy latami na zasilaniu bateryjnym. Infrastruktura ta powinna być dostępna nie tylko w modelu B2B dla dużych firm, powinna wspierać również sektor SME. W celu podjęcia decyzji biznesowych (w zakresie analityki czy optymalizacji, ubezpieczeń) niezbędne jest dostarczenie wystarczającej ilości stale aktualizowanych danych.

- Stworzenie na poziomie administracji państwowej ogólnie dostępnych zasobów informacji klimatycznej i hydrologicznej o dużej gęstości siatki – chodzi o rzeczywiste dane ze stacji pogodowych, punktów pomiarowych, nie będące wyłącznie symulacjami i prognozami.

- Zagwarantowanie dostępu do danych z wielu źródeł, otworzyć i bezpłatnie udostępnić zasoby systemów krajowych (w tym dane historyczne). Istotna jest duża dokładność oraz aktualność danych. W przypadku tworzenia nowych baz powinny zostać zapewnione mechanizmy informowania o współczynniku wiarygodności/dokładności danego źródła danych (uwzględnianie np. starzenia się czujników). Sugerujemy równoległe zapewnienie finansowania dla podmiotów publicznych w zakresie dostarczania i utrzymania takich baz oraz podnoszenia kompetencji instytucji w tej dziedzinie. Elementem infrastruktury jest również część informatyczna, związana z przechowywaniem i przetwarzaniem danych. Ważna jest metodyka gromadzenia danych, interoperacyjność danych oraz możliwość agregowania danych pochodzących z różnych źródeł w celach analitycznych i zastosowanie w tym zakresie istniejących, otwartych standardów. Dane z baz krajowych (realizowanych przez podmioty publiczne) powinny być dostępne dla użytkowników bezpłatnie.

- Finansowe wsparcie instalacji referencyjnych – farmy demonstracyjne (np. należące do ośrodków doradztwa rolniczego mających bezpośredni kontakt z klientami – rolnikami), wsparcie dla programów pilotażowych w zakresie IoT. Sugerujemy stworzenie ram prawnych dla partnerstwa publiczno-prywatnego dające możliwości łatwego testowania i demonstrowania pomysłów biznesowych.

- Stworzenie instytucjonalnych form finansowego wsparcia projektów IoT o szczególnym znaczeniu społecznym (gdzie zysk nie jest priorytetem): na przykład infrastruktura monitoringu smogu (gęsta sieć sensorów jakości powietrza w miastach, sensory na kominach, przy zakładach produkcyjnych, szlakach komunikacyjnych), zastosowanie IoT w pomiarach suszy, w gospodarce pasiecznej, hodowli, wsparcie racjonalnego stosowania środków ochrony roślin i nawozów w produkcji rolnej.

- Opracowanie dotowanych form edukacji w zakresie cyfrowej gospodarki, w tym IoT. Dokształcanie w zakresie technologii IoT dla instytucji typu ośrodki doradztwa rolniczego, instytuty naukowe związane z rolnictwem, uniwersytety przyrodnicze (dla propagatorów wiedzy).

SYSTEM NAWADNIANIA UPRAW

POLSKA

PROBLEM

Wysokie koszty nawadniania pól w okresach suszy.

ROZWIĄZANIE

Zintegrowany system nawadniania upraw iHorti dla średnio i wielkopowierzchniowych gospodarstw ogrodniczych. Zadaniem systemu jest:

1. Określenie optymalnej dawki nawodnieniowej dla danego fragmentu zagonu pola uprawnego w danym dniu dzięki układowi czujników monitorujących warunki środowiskowych, takie jak wilgotność gleby, ewapotranspiracja roślin uprawnych i gleby, nasłonecznienie, wiatr, opad naturalny, temperatura powietrza, ukształtowanie powierzchni pól uprawnych, przyrostu masy zielonej.

2. Nawadnianie oparte o deszczownie szpulowe ze zraszaczami obrotowymi bądź konsolami zraszającymi. Deszczownie wyposażone w sterowniki cyfrowe pozwalają na precyzyjne kontrolowanie podawanej dawki wody, pełne zdalne programowanie prac nawodnieniowych, geolokalizację zespołu nawadniającego w celu precyzyjnego podawania dawki wody w konkretnym fragmencie zagonu pola uprawnego, zbieranie danych o wykonanych pracach i zużyciu wody oraz innych parametrach systemu.

Współpraca obu tych komponentów z aplikacją centralną gwarantuje gospodarstwu ogrodniczemu możliwość scentralizowanego planowania i nadzorowania oraz optymalizacji prac nawodnieniowych w okresach dziennych, tygodniowych, sezonowych i wieloletnich.

KORZYŚĆ

Zmniejszenie zużycia wody na każdy hektar pola i kilogram plonu. Ochrona środowiska naturalnego poprzez ochronę zasobów wody. Optymalizacja kosztu produkcji żywności (warzyw).

15

TELEKOMUNIKACJA

Po prawie dwustu latach rozwoju telekomunikacji, która zmieniła świat i połączyła ludzi na całym świecie, branża telekomunikacyjna stoi przed kolejnym wyzwaniem. Połączenie miliardów urządzeń IoT może przyspieszyć tempo rozwoju gospodarczego i pomóc rozwiązać niektóre problemy naszej cywilizacji.

AUTORZY:
MATEUSZ MICHALSKI, MTECHNOLOGY /STOWARZYSZENIE HACKERSPACE WROCŁAW – LIDER PODGRUPY
TOMASZ DYLIK, EXATEL
JANUSZ GÓRSKI, T-MOBILE POLSKA S.A.
MAGDALENA KOGUT-CZARKOWSKA, ZWIĄZEK PRACODAWCÓW BRANŻY INTERNETOWEJ IAB POLSKA

Ogólna charakterystyka branży

Branża telekomunikacyjna pełni kluczową rolę w procesie wdrożenia i rozwoju Internetu Rzeczy. W oparciu o usługi świadczone przez branżę telekomunikacyjną możliwe jest szybkie realizowanie idei Internetu Rzeczy na szeroką skalę. Analogicznie jak miało to wcześniej miejsce w przypadku upowszechnienia dostępu do sieci Internet.

Od początków telekomunikacji, rozwiązania techniczne były głównie ukierunkowanie na realizację potrzeb człowieka, jako użytkownika końcowego usług. Obecnie rynek telekomunikacyjny zbliża się do masowego wdrożenia autonomicznych systemów opartych na urządzeniach, które będą komunikować się między sobą bez ingerencji człowieka, lub przy jej znikomej roli. Urządzenia te połączone w sieć, tworzą Internet Rzeczy, wprowadzając nowy rodzaj połączeń/ruchu w sieciach telekomunikacyjnych. Realizowany ruch ma inną charakterystykę oraz inne wymagania w porównaniu do ruchu generowanego przez użytkownika. Obecnie systemy IoT korzystają w większości przypadków z rozwiązań technologicznych, które pierwotnie zaprojektowano z myślą o człowieku jako odbiorcy. Twórcy urządzeń wykorzystują takie standardy jak GPRS, UMTS, WiFi, LTE, Ethernet i inne, do zapewniania łączności bezprzewodowej lub przewodowej z ich urządzeniami. Jednakże branża telekomunikacyjna przygotowała nowe standardy komunikacyjne odpowiadające na potrzebę wdrożenie masowego IoT.

Telekomunikacja bezprzewodowa dla IoT

Bezprzewodowe standardy telekomunikacyjne dla IoT odgrywają najważniejszą rolę jako technologie „ostatniej mili". Dzięki nim włączenie do sieci urządzeń IoT jest łatwiejsze i dostępne niemal wszędzie. Międzynarodowe organizacje przygotowały bezprzewodowe standardy zarówno dla pasm licencjonowanych, jak i dla pasm nielicencjonowanych. Są to standardy dla sieci typu LPWAN (ang. *Low Power Wide Area Network*), czyli bezprzewodowych niskoenergetycznych sieci dalekiego zasięgu.

Główne założenia będące podstawą stworzenia standardów dedykowanych dla IoT to:

- Energooszczędność – zapewniająca długą pracę na zasilaniu bateryjnym (nawet powyżej 10 lat),
- zwiększone pokrycie (zasięg) – umożliwiające instalację urządzeń w miejscach, w których obecnie nie jest to możliwe (piwnice, szyby windowe, lasy itp.),
- niski koszt modułów komunikacyjnych,
- niski koszt wdrożenia infrastruktury,
- wysoka pojemność sieci wspierająca *massive IoT*.

Standardy w paśmie licencjonowanym

1. **GSM, UMTS, LTE, NR**
   GSM/GPRS (ang. *Global System for Mobile Communications*), UMTS (ang. *Universal Mobile Telecommunications System*) i LTE (ang. *Long Term Evolution*) to powszechne cyfrowe standardy komórkowe. Każdy z nich potrafi przenosić zarówno głos, wiadomości tekstowe, wiadomości multimedialne, jak i dane pakietowe. Pomimo tego, że obecnie na tych standardach budowane są rozwiązania IoT, standardy te nie są optymalne dla Internetu Rzeczy. Szczególnie dla prostych urządzeń takich jak np. wodomierze. Żaden z tych standardów nie spełnia wszystkich wspomnianych wcześniej założeń, które powinien spełniać standard komórkowy dla IoT. W związku z czym, wdrożenie IoT na skalę masową jest ekonomicznie nieopłacalne. Standard NR (ang. *New Radio*), który będzie stanowił trzon sieci piątej generacji, również skupił się na bardzo szybkim przesyle danych, wychodząc z założenia, że połączenia IoT powinny być realizowane w innych technologiach. Dopiero na dalszych etapach rozwoju NR planowane jest wsparcie dla IoT, które miałoby zostać zrealizowane podobnie jak zrobiono to w LTE wprowadzając technologie takie jak Cat-M, NB-IoT, V2X, ProSe itd. Wyjątkiem są urządzenia związane z pojazdami autonomicznymi i innymi urządzeniami wymagającymi bardzo niskich opóźnień i wysokiej jakości transmisji. Te urządzenia będą zmuszone korzystać z najnowszych i najbardziej wydajnych rozwiązań należących do technologii LTE, 5G lub innej.

2. **NB-IoT**
   NB-IoT (ang. *Narrow Band – Internet of Things*) jest standardem komórkowym dla IoT pracującym w paśmie o szerokości 200 kHz. NB-IoT jest częścią systemu komórkowego LTE. Jednakże z punktu widzenia technicznego jest to nowa technologia dostępu radiowego. Nie istnieje kompatybilność pomiędzy urządzeniami NB-IoT a zwykłą siecią LTE. Sieć komórkowa NB-IoT może zostać uruchomiona na bazie istniejącej sieci LTE poprzez aktualizację oprogramowania w sieci operatora, co ma wpływ na koszt i czas wdrożenia. NB-IoT po stronie radiowej może zostać zaimplementowane na 3 różne sposoby, przy czym wszystkie mogą być wykorzystywane jednocześnie w obrębie jednej sieci radiowej. Komórki NB-IoT mogą zostać wydzielone wewnątrz komórek LTE (ang. *in-band mode*). Komórka NB-IoT może zostać także umieszczona obok komórki LTE w paśmie ochronnym (ang. *guard-band mode*). Jest to bardzo efektywne rozwiązanie, ponieważ nie wpływa na przepustowość macierzystej komórki, a korzysta z tego samego sprzętu co komórka macierzysta. Ostatnim sposobem uruchomienia komórki NB-IoT jest tryb samodzielny (ang. *standalone mode*), który umożliwia ponowne wykorzystanie kanałów częstotliwościowych ze standardu GSM/GPRS. Dla urządzenia końcowego nie ma znaczenia w jakim trybie działa sieć.

NB-IoT jest zaprojektowane dla prostych urządzeń, które nie wymagają wysokich przepływności danych, a także łączą się z siecią stosunkowo rzadko. Jest to propozycja dla aplikacji, które obecnie korzystają z sieci GSM/GPRS. Idealnym przykładem urządzeń, dla których technologia NB-IoT jest odpowiednia to urządzenia związane z opomiarowaniem, rolnictwem, logistyką, czujnikami pogodowymi, alarmami itp. NB-IoT zapewnia wysoką wydajność energetyczną pod warunkiem, że wysyłane dane są względnie małe (np. krótkie raporty zużycia, podniesienie alarmu, odczyty z sensorów) i raportowane są rzadko (kilka razy na dobę, lub rzadziej). W takich przypadkach żywotność baterii o pojemności 5Wh może przekroczyć nawet 30 lat. W przypadku wysłania większych ilości danych lub wysyłania ich często, bardziej wydajnym standardem może okazać się Cat-M. Standard NB-IoT zakłada również, że w obrębie jednej komórki przy założonym modelu ruchu, możliwe jest funkcjonowanie ponad 50 tyś. urządzeń IoT.

Kolejną kluczową możliwością standardu NB-IoT jest zwiększone pokrycie. NB-IoT oferuje ponad 20 dB zysku w pokryciu względem GSM/GPRS. Umożliwia to montaż urządzeń w miejscach w których obecne standardy komórkowe przestają działać np. szyby windowe, piwnice, studzienki, lasy itp. Niestety okupione jest to czasem życia baterii, osiąganą przepływnością danych, a także opóźnieniem. Opóźnienie w skrajnych przypadkach może wynosić kilka minut i wysłanie większej porcji danych może okazać się praktycznie niemożliwe.

Po okresie rozwojowym, koszt modułów radiowych NB-IoT powinien według założeń wynosić poniżej 5 dolarów amerykańskich. Aktualnie cena ta często przekracza 10 dolarów. Może to być kluczowy czynnik opóźniający wdrożenie standardu na masową skalę, ponieważ moduły GSM/GPRS już dawno osiągnęły cenę znacznie poniżej 5 dolarów.

3. **EC-GSM-IoT**
   EC-GSM-IoT (ang. *Extended Coverage GSM IoT*) to standard wprowadzający zmiany w funkcjonowaniu sieci GSM, dostosowując ją do wymagań IoT. To rozwiązanie korzysta z zasobów konwencjonalnej sieci GSM/GPRS dodając funkcjonalności wzorowane na NB-IoT takie jak zwiększone pokrycie, czy też energooszczędność. Dodatkowo wprowadza rozwiązania z zakresu bezpieczeństwa, które dotychczas były bolączką systemu drugiej generacji. Czas życia baterii przewidywany jest na podobnym poziomie do NB-IoT.

   Rozwiązanie to wymaga jedynie aktualizacji oprogramowania sieci GSM u operatora. Usługi EC-GSM-IoT to przesyłanie danych i wiadomości tekstowych, natomiast połączenia głosowe mogą być realizowane po przełączeniu się na konwencjonalny tryb GSM i nie mogą być realizowane w zwiększonym pokryciu. Podobnie jak NB-IoT w trybie in-band, EC-GSM-IoT wpływa negatywnie na pojemność komórki GSM dla konwencjonalnych usług. Zasoby radiowe dzielone są w czasie pomiędzy urządzenia EC-GSM-IoT i pozostałe urządzenia GSM. Pomimo tego, zakłada się, że w obrębie jednej komórki będzie mogło funkcjonować podobnie jak w NB-IoT ponad 50 tys. urządzeń IoT.

   Oczekuje się, że koszt modułu radiowego już na początku będzie niższy niż koszt modułu NB-IoT, w związku z bazowaniem na istniejących modułach GSM. Standard wydaje się więc idealnym kandydatem do szybkiego wdrożenia, jednak nie cieszy się on dużą popularnością. W praktyce operatorzy telekomunikacyjni z krajów europejskich oraz krajów, w których pokrycie siecią LTE jest zbliżone do pokrycia GSM, stawiają w pierwszej kolejności na rozwiązania bazujące na standardzie LTE. Być może standard ten rozwinie się później w krajach z dużą przewagą pokrycia GSM nad innymi technologiami.

4. **Cat-M**
   Cat-M (ang. *Category-M*), często nazywany też eMTC (ang. *Enhanced Machine-Type Communication*) lub LTE-M, jest standardem, który podobnie jak NB-IoT bazuje na sieci LTE, jednak nie jest rozpatrywany jako osobna technika dostępu radiowego. Cat-M jak nazwa wskazuje, uznaje się za specjalną kategorię terminala sieci LTE, który ma uproszczoną budowę i ograniczone możliwości względem innych kategorii występujących w LTE. Główna różnica to obsługiwana szerokość pasma, 1,4 MHz lub 5 MHz, względem standardowych bazujących na paśmie 20 MHz. Rozwiązanie Cat-M można umiejscowić jako technologia pomiędzy NB-IoT a LTE. Oznacza to, iż osiągane przepływności są znacznie większe niż w NB-IoT, ale również znacznie mniejsze niż w klasycznym LTE. Dodatkowo w porównaniu do NB-IoT w tym standardzie można realizować połączenia głosowe w technologii VoLTE, także w pewnym zakresie zwiększonego pokrycia względem LTE. Cat-M jest standardem przeznaczonym głównie dla tanich urządzeń mobilnych z małymi wymaganiami na przepływność danych (poniżej 1 Mb/s). Przykładowe urządzenia korzystające z Cat-M to bardzo tanie telefony LTE (głos i wiadomości), urządzenia monitorujące zdrowie i osoby starsze, terminale płatnicze i inne urządzenia IoT wymagające częstych połączeń i pozostające w ruchu.

   Do uruchomienia Cat-M w sieci operatora wystarczająca jest aktualizacja oprogramowania na stacjach bazowych i niektórych urządzeniach sieci szkieletowej. Technologia ta wspiera wszystkie rozwiązania energooszczędności znane z NB-IoT, a także zwiększone pokrycie, które pierwotnie miało wynosić ok. 12 dB w porównaniu do GSM, jednak wiele opracowań wskazuje, że Cat-M jest w stanie zbliżyć się do 20 dB zysku podobnie jak NB-IoT. Żywotność baterii dla prostych aplikacji przekracza 10 lat, pod warunkiem zachowania dobrych warunków radiowych.

OPTYMALIZACJA ODBIORU ŚMIECI OPARTA NA LORAWAN

HISZPANIA

PROBLEM

Regularny odbiór śmieci, po ustalonej na sztywno trasie jest nieoptymalny i powoduje zbędne generowanie kosztów i spalin.

ROZWIĄZANIE

W Hiszpanii, w prowincji Salamanka, wdrożono system optymalizujący proces odbioru śmieci oparty na standardzie LoRaWAN*. W pojemnikach na śmieci zainstalowano czujniki, które raportowały stan napełnienia koszy do systemu centralnego. Na podstawie tych danych, system przygotowywał optymalne trasy przejazdu śmieciarek.

KORZYŚĆ

Znaczne obniżenie kosztu odbioru śmieci i zmniejszenie zanieczyszczenia powietrza poprzez obniżenie emisji spalin. Przed wdrożeniem systemu, pojazdy odbierające śmieci pokonowały codziennie dystans około 3050 km. Po uruchomieniu systemu, sumaryczny dystans uległ skróceniu średnio o ok. 1076 km.

* *„Smart Waste Collection System with Low Consumption LoRaWAN Nodes and Route Optimization” https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5982603/*

Standardy w paśmie nielicencjonowanym

1. **LoRaWAN**

LoRaWAN jest standardem stworzonym przez konsorcjum *LoRa Alliance*. Jest to standard pracujący w pasmach ISM poniżej 1 GHz. W Europie system ten pracuje w paśmie 433 lub 868 MHz. Podobnie jak NB-IoT, LoRaWAN jest standardem dla sieci typu LPWAN. Jest to standard nastawiony na transmisję małych porcji danych od urządzeń końcowych. Standard ten oferuję przepływności niższe niż NB-IoT, także z rzadszą możliwością połączeń i niższą gwarancją, co spowodowane jest wymaganiami dla pasm ISM. Zastosowania LoRAWAN są w zdecydowanej większości takie same jak NB-IoT, dlatego wprost można rozważać ten standard jako konkurencyjny wobec NB-IoT, w zastosowaniach niewymagających wysokiej gwarancji zasobów.

Specyfikacja LoRaWAN nastawiona jest na proste rozwiązania radiowe, które umożliwiają znaczne obniżenie kosztów produkcji samych modułów radiowych. Dłuższy rozwój w porównaniu do komórkowych odpowiedników skutkuje w chwili obecnej znacznie niższymi kosztami modułów radiowych. Standard w zależności od opracowań zapewnia warunki radiowe łącza od 10 do 20 dB wyższy niż GSM, czyli podobnie jak NB-IoT i CaT-M.

Sieci LoRaWAN mogą być tworzone przez organizacje non-profit oraz użytkowników prywatnych na podstawie ogólnie dostępnych urządzeń, podobnie jak ma się to do standardu Wi-Fi. Standardem interesuję się też operatorzy telekomunikacyjni, którzy chcieliby wykorzystać go w ramach komercyjnych usługii.

2. **SigFox**

SigFox jest standardem dla sieci typu LPWAN. Jest to standard częściowo zamknięty. Dopiero od 13 stycznia 2019 roku, otwarto radiową część standardu pozwalającą na tworzenie własnych implementacji urządzeń końcowych. Właściciel standardu buduje własne sieci dostępowe samodzielnie lub na zasadzie partnerstwa z lokalnymi operatorami. W Polsce sieci SigFox nie są jeszcze dostępne, chociaż według doniesień medialnych firma jest zainteresowana wejściem na rynek polski w najbliższym czasie.

ODCZYT CIEPŁOMIERZY OPARTY NA NB-IoT

POLSKA

PROBLEM

Wysokie koszty odczytu ciepłomierzy na terenie czterech gmin: Białego Dunajca, Poronina, Szaflar i Zakopanego.

ROZWIĄZANIE

T-Mobile Polska we współpracy z firmą ABARO wdrożył dla Przedsiębiorstwa Energetyki Cieplnej Geotermia Podhalańska S.A., największej w Polsce firmy wytwarzająca ciepło z energii geotermalnej, kompletny system automatycznego odczytu ciepłomierzy oparty na technologii NB-IoT. Dzięki temu rozwiązaniu Geotermia jest pierwszą w Polsce siecią ciepłowniczą, w której zdalny odczyt w całości został oparty o technologię transmisji NB IoT.
W ramach kontraktu T-Mobile wspólnie z ABARO dostarczył ponad 1500 urządzeń telemetrycznych oraz zapewnił pełną infrastrukturę telemetryczną (transmisje danych NB-IoT, serwery, oprogramowanie, wsparcie technicznie i usługi serwisowe).

KORZYŚĆ

Dzięki częstemu, automatycznemu, zbieraniu najważniejszych danych z całej sieci ciepłowniczej, projekt umożliwił optymalizację zużycia energii oraz zwiększenie komfortu obsługi klientów.

Standard ten pracuje na paśmie ISM 868 MHz. SigFox bazuje na bardzo krótkich wiadomościach. Użyteczna porcja danych, która może zostać przesłana w ramach jednej wiadomości to tylko 12 oktetów. Ze wszystkich opisanych w tym rozdziale standardów bezprzewodowych jest to standard o najmniejszych możliwościach transmisyjnych. Zastosowanie SigFox to przede wszystkim bardzo proste urządzenia typu czujniki, czy też tagi geolokalizacyjne.

3. **Inne**

Wyżej opisano najpopularniejsze standardy dla sieci LPWAN, oczywiście na świecie istnieją inne standardy komunikacyjne, jednak nie są one na tyle popularne, żeby stanowiły przedmiot rozprawy w niniejszym raporcie.

Wszystkie standardy krótkozasięgowe takie jak Bluetooth, ZigBee oraz inne, traktowane są przez branżę telekomunikacyjną jako standardy dedykowane pod konkretne systemy i w głównej mierze o lokalnym zasięgu. Z racji tego, że nie mają predyspozycji do stania się usługami publicznie dostępnymi, również nie stały się przedmiotem rozważań grupy.

Telekomunikacja przewodowa i infrastruktura

Podobnie jak krótko-zasięgowa łączność bezprzewodowa, wszystkie standardy przewodowe dla IoT uznaje się za rozwiązania dedykowane pod indywidualne potrzeby, o zasięgu lokalnym. Wyjątkiem mogłaby być technologia przesyłania danych przez sieci elektryczne, jednak w ramach prac grupy nie zidentyfikowano konkretnych potrzeb dla tej techniki.

Uruchomienie bezprzewodowych sieci typu LPWAN i 5G, może wiązać się z koniecznością rozbudowy infrastruktury telekomunikacyjnej, wliczając w to infrastrukturę szkieletową sieci oraz budowę nowych punktów dostępowych i stacji bazowych. Szczególnie technologia 5G potencjalnie może wymagać instalacji wielu nowych stacji bazowych, także w miejscach, które nie są obecnie oczywiste. Z punktu widzenia branży, ważne jest, żeby polskie regulacje prawne nie hamowały szybkiej rozbudowy infrastruktury telekomunikacyjnej, co jednocześnie mogłoby skutkować opóźnieniem w powszechnym wdrożeniu 5G w Polsce.

Perspektywa rozwoju branży

Firma Ericsson w wydanym przez siebie w listopadzie 2018 roku raporcie o telekomunikacji mobilnej (ang. *Ericsson Mobility Report*) szacuje, że do 2024 roku ilość urządzeń IoT na świecie będzie rosnąć w tempie 17% rocznie (skumulowany roczny wskaźnik wzrostu) osiągając 22,3 mld urządzeń z początkowych 8,6 mld w 2018 roku:

Ilość urządzeń IoT w miliardach

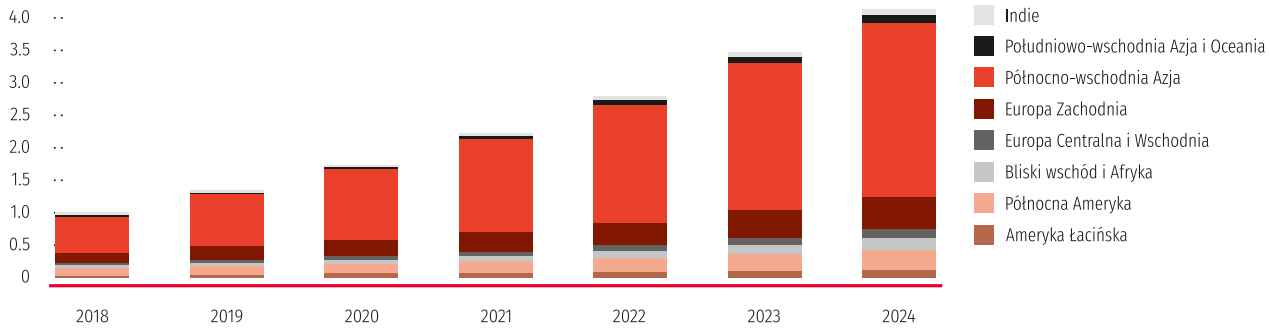
IoT	2018	2024	CAGR
IoT daleko-zasięgowe (LPWAN)	1.1	4.5	27%
⇨ IoT komórkowe	1.0	4.1	27%
IoT krótkozasięgowe	7.5	17.8	15%
Suma	**8.6**	**22.3**	**17%**

Źródło: Ericsson Mobility Report November 2018

Największe tempo wzrostu przewidywane jest dla połączeń daleko-zasięgowych (LPWAN), których motorem napędowym ma być wdrożenie komórkowego IoT. Krótko-zasięgowa oraz przewodowa komunikacja IoT będzie rosnąć w tempie 15% rocznie.

Na załączonym poniżej diagramie przedstawiono prognozowaną ilość urządzeń podłączonych w standardach komórkowego IoT w danym roku z podziałem na regiony świata. Jak można zaobserwować, nie przewiduje się znaczącej zmiany proporcji w podziale rynku pod względem ilości podłączonych urządzeń, co sugeruje podobny wzrost rynku na całym globie.

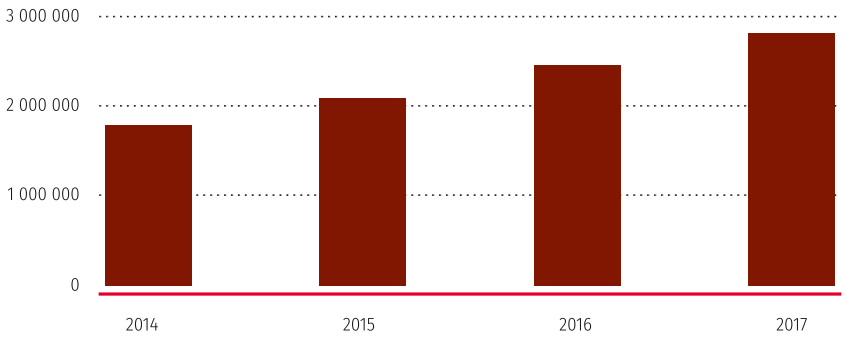
Liczba podłączonych urządzeń komórkowego IoT według regionu [w miliardach]



Źródło: Ericsson Mobility Report November 2018

Na wykresie poniżej przedstawiono ilość kart SIM oficjalnie uznanych przez operatorów za M2M w latach 2014–2017. Dane zostały pozyskane ze sprawozdań składanych do Prezesa UKE przez operatorów telekomunikacyjnych. W roku 2017 liczba kart SIM sklasyfikowanych jako karty do komunikacji M2M, wynosiła ok. 2,8 mln kart SIM.

Liczba kart M2M w Polsce



Źródło: Wykres własny na podstawie danych z Urzędu Komunikacji Elektronicznej

Gdyby przyjąć tempo wzrostu szacowane przez firmę Ericsson oraz liczbę kart oficjalnie uznanych w Polsce za M2M, to w roku 2024 w Polsce powinniśmy osiągnąć ok. 12 mln aktywnych kart SIM typu M2M. Z danych udostępnianych przez UKE wynika, że rynek komunikacji ruchomej w Polsce uległ nasyceniu i nie wliczając kart M2M wynosi ok. 50 mln subskrybcji. Oznacza to, że gdyby ta ilość utrzymała się na podobnym poziomie do 2024 roku, to ilość kart M2M na polskim rynku mogłaby stanowić około 20% w stosunku do wszystkich kart SIM. Niewiadomą pozostaje liczba „ukrytych" kart M2M, które w raportach ukryte są w liczbie zwykłych subskrypcji. Bazując jednak tylko na oficjalnej liczbie kart M2M, można stwierdzić, że trzecia dekada XXI wieku będzie dla branży telekomunikacyjnej oprócz rozwoju 5G, rozwojem IoT.

Obecnie w Polsce komórkowe technologie dla IoT zostały wdrożone częściowo w T-Mobile Polska, które pokryło pewien obszar swojej sieci zasięgiem NB-IoT, a także przez Orange Polska, które testuje w kilku lokalizacjach technologię Cat-M. W niektórych miastach prywatne firmy lub organizacje udostępniły punkty dostępowe LoRaWAN. Daje to szanse na realne wprowadzenie powszechnego dostępu do usług komórkowego IoT na terenie Polski w najbliższych latach.

Zakres możliwego wykorzystania IoT

Branżę telekomunikacyjną można rozumieć jako branżę zajmującą się tylko usługą przesyłania danych. W związku z czym, to od użytkowników z innych sektorów przemysłu będzie zależało wykorzystanie potencjału świadczonych przez branżę telekomunikacyjną usług i nadanie im ostatecznego kształtu. Z drugiej strony, obecna sytuacja rynkowa często powoduje, że odbiorcy rozwiązań IoT zainteresowani są całościowym rozwiązaniem dla swojej branży i to operatorzy telekomunikacyjni jako podmioty agregujące produkty innych podmiotów, mogą oferować gotowe rozwiązania dla innych sektorów przemysłu.

Bariery

W toku prac grupa zidentyfikowała następujące obszary barier dla branży telekomunikacyjnej:

1. Ograniczona dostępność infrastruktury telekomunikacyjnej spełniającej wymagania IoT na masową skalę.

2. Normy PEM znacznie bardziej restrykcyjne niż średnia w UE ograniczają rozwój technologii 5G i IoT opartych na sieciach komórkowych.

3. Ograniczone zasoby finansowe do przeprowadzenia niezbędnych inwestycji w infrastrukturę na szeroką skalę.

4. Niedostosowanie przepisów prawnych do komunikacji urządzeń typu IoT/M2M.

5. Ograniczenia regulacyjne w zakresie analityki opartej na dużych zbiorach danych.

Propozycje działań rządu

Podstawowym aktem prawnym regulującym sektor telekomunikacyjny jest prawo telekomunikacyjne. Wraz ze wzrastającym znaczeniem usług teleinformatycznych dla różnych sektorów gospodarki kraju, wzrasta zakres norm, przepisów, regulacji mających wpływ na przedsiębiorstwa telekomunikacyjne. Dotyczy to zarówno kwestii przetwarzania danych, bezpieczeństwa świadczonych usług, czy też warunków świadczenia usługi dostępu do sieci Internet.

Charakterystycznym zjawiskiem jest coraz większa złożoność przepisów prawnych oraz ich sprzeczność, które de facto stają się barierą dla nowych innowacyjnych usług IoT. W szczególności, gdy usługi komunikacji postrzegane są jako element składowy samego urządzenia IoT.

Dodatkowo, przepisy prawne są ukierunkowane na świadczenie usług telekomunikacyjnych dedykowanych do komunikacji interpersonalnej. Z tego powodu szereg przepisów prawnych, w sposób szczegółowy regulują relację z osobą fizyczną, które nie mają znaczenia w przypadku komunikacji urządzeń IoT.

W związku z tym, konieczne jest dostosowanie przepisów prawnych do specyficznych uwarunkowań komunikacji IoT. Dobrym momentem na przeprowadzenie tych zmian jest realizowany obecnie proces wdrożenia do przepisów krajowych Europejskiego Kodeksu Łączności Elektronicznej.

Drugim kluczowym aktem prawnym mającym istotne znaczenie dla komunikacji IoT jest projekt rozporządzenia ePrivacy, który bezpośrednio dotyka zagadnień związanych z przetwarzaniem danych wytwarzanych w sieci telekomunikacyjnej przez urządzenia IoT.

W związku z powyższym grupa rekomenduje następujące działania:

1. Dostosowanie polskich norm dotyczących promieniowania elektromagnetycznego (PEM) do warunków, jakie panują w innych krajach członkowskich UE. Umożliwi to rozbudowę i modernizację radiowej sieci telekomunikacyjnej, która jest fundamentem dla świadczenia złożonych usług IoT. Dodatkowo, przyszłe różnorodne oczekiwania warunków świadczenia usług IoT przez operatorów, ukierunkuje inwestycje na wdrożenie sieci 5G.

2. Mając na uwadze złożoność otoczenia regulacyjnego, które zostało zbudowane na potrzeby komunikacji interpersonalnej, rekomendujemy stworzenie definicji legalnej pojęcia urządzenia/użytkownika IoT, który następnie pozwoli na dostosowanie (tj. zmniejszenie) zakresu obowiązków regulacyjnych dla komunikacji IoT. Dotyczy to w szczególności przepisów prawnych dotyczących relacji interpersonalnych tj. billing szczegółowy, przenoszalność numerów, czas trwania kontraktu, realizacji połączenia na numery

WDROŻENIE CELLULAR IoT I NIDD

JAPONIA

PROBLEM

Ryzyko ataków na systemy IoT dostępne przez protokół IP.

ROZWIĄZANIE

Japoński operator komórkowy SoftBank jesienią 2018 r. przeprowadził udane testy połączeń typu NIDD* (ang. *Non-IP Data Delivery*), które umożliwiają wymianę danych bez alokacji adresu IP dla urządzenia (docelowo także numeru telefonu). Połączenia zostały wykonane w komercyjnie działającej sieci w standardzie NB-IoT.

KORZYŚĆ

Ograniczenie ryzyka wrogich ataków na urządzenia IoT, prowadzonych w sieciach IP i stworzenie bezpiecznego połączenia od urządzenia aż po infrastrukturę przetwarzającą dane. Dzięki usunięciu narzutu generowanego przez protokół IP, proste urządzenia NB-IoT mogą zyskać na żywotności baterii. Przykład japońskiego operatora prezentuje wzorcowy proces przygotowywania infrastruktury telekomunikacyjnej na *massive IoT.*

* *„SoftBank Launches World's First Experimental Services in Commercial Environment Using NIDD Technology for NB-IoT" https://www.softbank.jp/en/corp/group/sbm/news/press/2018/20180928_01/*

alarmowe, adresacja urządzeń bez użycia numerów telefonicznych itp.

3. Rozpoczęcie dialogu z operatorami telekomunikacyjnymi na temat wprowadzenia technologii przenoszenia kart eSIM, jako alternatywy dla przenoszenia numerów w zastosowaniach IoT. Potrzeba ta jest motywowana niemożliwością fizycznej wymiany kart eSIM w tysiącach urządzeń, których żywotność może przekroczyć 10 lat.

4. Zmniejszenie restrykcyjnych wymagań dotyczących wykorzystania dużych zbiorów danych wytwarzanych przez urządzenia IoT w sieciach telekomunikacyjnych. W szczególności, należy wyraźnie wskazać, iż po przeprowadzeniu anonimizacji/pseudonimizacji dane mogą być wykorzystywane na inne potrzeby.

5. Dbanie o utrzymanie otwartości przepływu danych przynajmniej w ramach grupy państw Europejskiego Obszaru Gospodarczego.

6. Usunięcie barier administracyjnych ograniczających rozwój infrastruktury telekomunikacyjnej – przykładem może być nowelizacja ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz rozszerzenie jej o budowę masztów/anten telekomunikacyjnych, czego wymagać będą technologie z rodziny 5G.

7. Umożliwienie powszechnego dostępu do danych będących własnością państwa i zbieranych w ramach systemów teleinformatycznych ufundowanych z pieniędzy publicznych np. inteligentne systemy transportu miejskiego, monitoring parkingów miejskich itp.

16

TRANSPORT, LOGISTYKA I POJAZDY AUTONOMICZNE

W obliczu obecnych wyzwań stawianych branży transportowej i coraz większej liczby podróży i dostaw, implementacja technologii IoT jest kluczowa.

AUTORZY:
LIDERZY PODGRUPY: PAWEŁ GORA, UNIWERSYTET WARSZAWSKI
DAMIAN HAJDUK, DORADZTWO I ZARZĄDZANIE W TRANSPORCIE I LOGISTYCE

ORAZ:
ŁUKASZ GAWLICZEK, AVE CARGO SP. Z O.O.
AGATA HORZELA, GS1 POLSKA
ANNA KONERT, UCZELNIA ŁAZARSKIEGO
TOMASZ KOSIŁO, POLITECHNIKA WARSZAWSKA
KONRAD KOSTRZEWA, VETURAI AUTOMOTIVE SP. Z O.O.
MAGDALENA KRYSTYNIECKA-KONOPCZAK, PLL LOT S.A.
KAROLINA KRZYKOWSKA, POLITECHNIKA WARSZAWSKA
BARTOSZ MAZUR, GOP GEAR, FUNDACJA „NAPRAW SOBIE MIASTO"
RADOSŁAW MOSKWA, CM LOGISTIC
PIOTR PRZECHERSKI, OLCZAK-KLIMEK, VAN DER KROFT, WĘGIEŁEK KANCELARIA RADCÓW PRAWNYCH SPÓŁKA PARTNERSKA
GRZEGORZ WILCZEWSKI, DAWIS IT SP. Z O.O.
EWA WOLNIEWICZ-WARSKA, KAPSCH TELEMATIC SERVICES SP. Z O.O.

KONSULTACJA MERYTORYCZNA:
MAŁGORZATA DAROWSKA, MINISTERSTWO INFRASTRUKTURY
MICHAŁ KLUSEK, GŁÓWNY URZĄD GEODEZJI I KARTOGRAFII
ZBIGNIEW MALINOWSKI, RADA INFRASTRUKTURY INFORMACJI PRZESTRZENNEJ, GEO-SYSTEM SP. Z O. O.

„Marzy się nam transport, w którym każdy użytkownik dysponuje własnym lekkim i ekologicznym środkiem transportu osobistego, korzystającym z odnawialnego źródła energii, dopasowaną do objętości człowieka ze standardowo niewielkim zapasem, umożliwiającym umieszczenie małego bagażu podręcznego. Nazwijmy go kapsułą. Kapsuła porusza się wolno na pierwszej i ostatniej mili, całkowicie samodzielnie. Kapsułę można zdemontować i zamontować w ciągu sekund z/do postaci przenośnej, wielkości małej damskiej torebki. Kapsułę możemy też nazwać samochodem. Kapsuły mogą łączyć się w zespoły kapsuł poruszające się nieco szybciej w dowolnej dostępnej konfiguracji o limicie górnym na punktach integracji pierwszego stopnia. Nazwijmy je autobusami i przystankami. Na potrzeby ewentualnej dalszej podróży zespoły kapsuł z przystanków przesiadkowych formowane są w jeszcze szybszy skład dalekobieżny na punkcie integracji drugiego stopnia. Nazwijmy je stacjami i pociągami. Podróże na jeszcze dalsze, duże odległości obsługiwane są przez specjalne, bardzo szybkie pojazdy, napełniane przez kapsuły na węzłach integrujących trzeciego stopnia. Nazwijmy je statkami i portami. (...)" (z prac podgrupy TLPA)

Ogólna charakterystyka branży

Transport rozumiany jest jako zorganizowane przemieszczanie ludzi (transport pasażerski) lub ładunków (transport towarowy/cargo) z jednej lokalizacji do drugiej. Sprawne funkcjonowanie transportu jest niezbędne do zapewnienia efektywnego rozwoju całej gospodarki, ale z transportem powiązane są również zagrożenia incydentami (kolizjami, wypadkami) i negatywnym wpływem na środowisko. Szacuje się, że wszyscy pracujący i podróżujący do/z pracy transportem indywidualnym w 7 największych miastach w Polsce tracą rocznie z powodu niewydolności systemu transportu ok. 3,6 mld PLN. Np. w Warszawie średni czas podróży jest o 38% dłuższy niż mógłby być, gdyby na drogach nie występowały utrudnienia. Natomiast podczas porannego i popołudniowego szczytu komunikacyjnego czas podróży wydłuża się odpowiednio o 66 i 73%. Światowa Organizacja Zdrowia (WHO), szacuje, że każdego roku w wypadkach drogowych ginie około 1,25 mln osób. W obliczu obecnych wyzwań stawianych branży transportowej, coraz większej liczby podróży i dostaw generowanych w efekcie rozwoju gospodarczego, inwestycji, zwiększonej konsumpcji dóbr i usług, implementacja technologii IoT jest kluczowa. Największym wyzwaniem branży transportowej w kontekście IoT jest organizacja otwartych, ustandaryzowanych interfejsów pozwalających na szeroką integrację, a także przygotowanie infrastruktury do przesyłania, przechowywania i przetwarzania dużej ilości danych generowanych przez IoT.

Obecnie transport może odbywać się w pięciu środowiskach: na lądzie (transport lądowy), pod lądem, na wodzie lub (rzadziej) pod nią (transport wodny), w powietrzu (transport powietrzny) i w przestrzeni kosmicznej. IoT może znaleźć zastosowanie w każdym z tych środowisk, ale biorąc pod uwagę liczbę pojazdów, powszechność ich używania i możliwe korzyści związane z IoT, obecnie kluczowy jest przede wszystkim transport lądowy i transport powietrzny. W każdym ze środowisk możliwe jest wykorzystywanie różnych środków transportu, np. w transporcie lądowym mogą być to np. pociągi, tramwaje, samochody, ciężarówki, autobusy, skutery, rowery lub ruch pieszy. W niniejszym rozdziale skupiamy się na tych środkach transportu oraz zagadnieniach transportowych, w których IoT może potencjalnie przynieść w najbliższych latach największy przełom i najwięcej korzyści.

Perspektywa rozwoju branży

Transport i logistyka na świecie przeżywają w ostatnich latach rozwój ilościowy, korzystając ze sprzyjających warunków, do których można zaliczyć:

1. Dobrą koniunkturę gospodarczą w drugiej połowie obecnej dekady.

2. Sukcesywny wzrost wolumenu handlu światowego (mimo przeciwstawnych trendów protekcjonistycznych).

3. „Fizyczne" zbliżanie się rynków Eurazji dzięki działaniom służącym poprawie sprawności funkcjonowania transportu w relacjach Daleki Wschód (Chiny) <-> Europa (UE):

    - rosnące perspektywy transeurazjatyckich szlaków lądowych uwidaczniają się wyraźnie po latach (wiekach) dominacji szlaków morskich,

    - inicjatywa Nowego Jedwabnego Szlaku (*One Belt One Road*) jako narzędzie partnerstwa i współpracy kontynentalnej, czy ekspansji chińskiej.

Wspólny Rynek Unii Europejskiej, a szerzej – Europejskiego Obszaru Gospodarczego – stał się motorem mobilności, wymiany towarowej, przepływu usług i łańcuchów dostaw (wartości) na Starym Kontynencie. Wymiana gospodarcza, mimo wciąż słyszalnego echa kryzysu południa Europy, napięć politycznych i ekonomicznych (w tym niejasnych perspektyw Brexitu) oraz zagrożeń zewnętrznych i wewnętrznych dla krajów wspólnego rynku, stale się zwiększa.

Gospodarka polska w kontekście transportu, logistyki i procesów ich automatyzacji i autonomizacji pozostaje w stanie dualizmu gospodarczego. Świat, a szczególnie Europa, stawiając coraz mocniej na podejście terytorialne i wielomodalne, wiąże różne gałęzie i środki transportu do zintegrowanej terytorialnie i funkcjonalnie usługi. Tymczasem w Polsce dość uporczywie kultywowane jest podejście jednomodalne (planowanie gałęziowe, mikroskopowość). Krajowa flota transportowa (ale tylko drogowa!) podbija Europę, natomiast wyraźnie mniejsza jest dynamika i oferta wewnętrzna transportu multimodalnego, zwłaszcza komponentu kolejowego, szczególnie uwzględniając nasze położenie, chociaż

w ostatnich latach również odnotowujemy tutaj ilościowy i jakościowy wzrost.

Rozwój gospodarczy to nie tylko konsumpcja, ale i inwestycje, które pomagają wykorzystać położenie geograficzne na szlakach będące przez wiele lat problemem, a obecnie stające się szansą. Dużym programom infrastrukturalno-cywilizacyjnym jak rozbudowa portów morskich (Port Centralny), czy mega-program Centralnego Portu Komunikacyjnego towarzyszą niezdecydowane, niespójne działania na rzecz przełamania w dużej mierze nieadekwatnego XIX wiecznego układu sieci komunikacyjnych. Od czasu do czasu wyłaniają się niezgodne z logiką gospodarki i sieci osadniczej działania i koncepcje konserwujące (a nawet potęgujące) dysfunkcjonalność sieci transportowej kraju, szczególnie widoczne w Polsce zachodniej.

Brak konsekwentności decyzyjnej widoczny jest szczególnie w kontekście zawirowań wokół programu budowy planowanej sieci kolei dużych prędkości. Nie jest także jednoznacznie rozstrzygalne z poziomu obecnego raportu na ile deklaratywne, a na ile realne są plany rządowe modernizacji kraju i gospodarki w kierunku przemysłu 4.0, szczególnie w zakresie transportu i logistyki. Oprócz wspomnianych deficytów i zbytecznych ograniczeń w organizacji i planowaniu, brakuje zintegrowanego podejścia do kształcenia kadr. Nowoczesny przemysł, w tym transport, logistyka i ich automatyzacja i autonomizacja od prostych urządzeń dnia (transportu) codziennego po poziom ekspansji kosmicznej, wymagają kompetencji systemowych i dostępności wykształconych kadr.

Zachodzące zmiany w różnych gałęziach transportu koncentrują się na rozszerzaniu mobilności ludzi jednocześnie zwiększając bezpieczeństwo, efektywność i trwałość samego transportu. Szczególną uwagę zwraca się na rozwój technologii cyfrowych (np. automatyzacji transportu), które będą bazować na warstwie danych, zawierających dane statyczne (mapy cyfrowe czy przepisy ruchu drogowego) oraz dane dynamiczne (informacje o warunkach i ruchu w czasie rzeczywistym). Technologie cyfrowe przyczyniają się do ograniczenia błędów ludzkich, będących najważniejszą przyczyną wypadków w transporcie. Mogą także przyczynić się do powstania multimodalnego systemu transportowego łączącego wszystkie rodzaje transportu w jedną zintegrowaną usługę, która będzie umożliwiać sprawny przewóz ludzi i ładunków *„od drzwi do drzwi”*. Również w Europejskiej strategii na rzecz mobilności niskoemisyjnej, zatwierdzonej w lipcu 2016 r.[1], zwraca się uwagę na rozwój usług integrujących pojazdy współpracujące, połączone i zautomatyzowane, w których widzi się potencjał w zakresie zmniejszania zużycia energii i emisji spalin. W niedalekiej przyszłości takie usługi będą ściśle współdziałać ze sobą, np. pojazdy będą mogły komunikować się między sobą (V2V – *vehicle-to-vehicle*), z infrastrukturą drogową (V2I – *vehicle-to-infrastructure*), z pieszymi uczestnikami ruchu (V2P – v*ehicle-to--pedestrian*) i z siecią teleinformatyczną (V2N – *vehicle--to-network*). Będzie to skoordynowane działanie umożliwiające użytkownikom dróg i zarządzającym ruchem wymianę informacji i interoperacyjność ich działań. Pojazdy współpracujące będą mogły tworzyć Internet Pojazdów (*Internet of Vehicles*) i ostrzegać siebie nawzajem o potencjalnie niebezpiecznych sytuacjach (np. nagłe hamowanie, wypadek, zablokowana droga), synchronizować swoje plany, trasy i manewry celem zapewnienia efektywności i bezpieczeństwa jazdy. Będzie też możliwa komunikacja pojazdów z infrastrukturą transportu, np. w celu przesłania pojazdom optymalnej trasy lub prędkości, bądź w celu umożliwienia lepszego zarządzania ruchem (np. wykrywanie zatorów, wypadków lub złych warunków, adaptacje ustawień sygnalizacji świetlnej). Duże ilości danych zbierane z przemieszczających się pojazdów będą mogły posłużyć jako źródło cennej wiedzy dla algorytmów sztucznej inteligencji umożliwiających lepsze niż obecnie planowanie sieci transportowych i optymalne zarządzanie nimi w czasie rzeczywistym. Połączenie pojazdów z siecią teleinformatyczną ułatwi z kolei pasażerom pracę, odpoczynek lub rozrywkę w trakcie podróży, co może mieć również istotne znaczenie dla gospodarki.

Testy związane z technologią C-ITS (Cooperative Intelligent Transportation Systems – współpracujące inteligentne systemy transportowe, komponenty sieci transportowej współpracujące ze sobą poprzez wymianę danych) prowadzone są już z powodzeniem przez wiele firm i krajów od wielu lat. Holandia, Austria i Niemcy stały się pierwszymi krajami europejskimi z komunikacją V2I w korytarzu C-ITS (C-ITS Corridor). Nad technologią pojazdów wyposażonych w komunikację V2X (*vehicle-to--everything*) pracowały już m.in. takie firmy jak: Toyota, Volkswagen, Volvo, Mercedes. Technologia V2X będzie szczególnie przydatna w erze pojazdów autonomicznych sterowanych przez program komputerowy, a nie przez człowieka, gdyż będzie mogła dać dodatkowo możliwości bezpieczniejszej i efektywniejszej jazdy. Prace nad pojazdami autonomicznymi prowadzi od wielu lat większość firm z branży motoryzacyjnej, ale także firmy informatyczne. Jednym z liderów jest firma Waymo, która pod koniec 2018 roku uruchomiła pierwszą komercyjną usługę (częściowo) autonomicznych taksówek. W 2019 roku w Szwecji autonomiczny pojazd elektryczny T-Pod uzyskał pozwolenie na poruszanie się po drogach publicznych i na początku będzie kursował między magazynem i terminalem. Trwają też prace nad autonomizacją innych środków transportu, np. kolejowego.

1 Europejska strategia na rzecz mobilności niskoemisyjnej, COM(2016) 501 final.

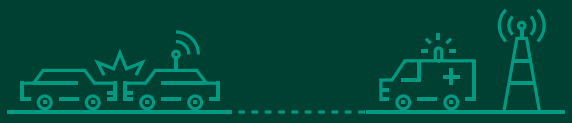
W europejskiej strategii na rzecz współpracujących inteligentnych systemów transportowych (COM (2016) 766) wyszczególniono usługi, które będą wymagały tzw. szybkiego wdrożenia (lista dnia 1) oraz usługi wdrożone w drugiej fazie, w przypadku których specyfikacje i normy mogą nie być dokończone (lista usług dnia 1.5).

Rozwiązanie	Opis	Korzyści
Lista usług C-ITS dnia 1	1.1. Powiadomienie o niebezpiecznej lokalizacji	Ostrzeżenie o powolnych lub stojących pojazdach i ruchu z przodu.
		Ostrzeżenie o robotach drogowych.
		Warunki pogodowe.
		Światło hamowania awaryjnego.
		Zbliżanie się pojazdu uprzywilejowanego.
		Inne niebezpieczeństwa.
	1.2. Zastosowanie oznakowania	Oznakowanie pokładowe pojazdu.
		Pokładowe ograniczenia prędkości pojazdu.
		Naruszenie sygnału / bezpieczeństwo skrzyżowań.
		Prośba pojazdów oznakowanych o pierwszeństwo sygnalizacji ruchu.
		GLOSA (Green Light Optimal Speed Advisory) rekomendacja prędkości celem przejazdu na zielonym świetle.
		Dane z sond pojazdu.
		Tłumienie fali uderzeniowej.
Lista usług C-ITS dnia 1.5		Informacje na temat stacji paliw i ładowania pojazdów z napędem alternatywnym.
		Ochrona niezmotoryzowanych użytkowników przestrzeni współdzielonej.
		Zarządzanie parkowaniem na ulicy i informacje w tym zakresie.
		Informacje o parkowaniu poza ulicą.
		Informacje dotyczące systemów „parkuj i jedź”.
		Nawigacja pojazdów połączonych i współpracujących do i z miasta.
		Informacje o ruchu i inteligentne wyznaczanie tras.

SYSTEM SZYBKIEGO POWIADAMIANIA O WYPADKACH DROGOWYCH eCALL

HTTPS://WWW.IRISHTIMES.COM/NEWS/IRELAND/IRISH-NEWS/NEW-CARS-TO-AUTOMATICALLY-INFORM-AUTHORITIES-OF-CRASHES-1.3447079

EUROPA



PROBLEM

Automatyczne wykrywanie wypadków i informowanie odpowiednich służb.

ROZWIĄZANIE

Od 1.04.2018 we wszystkich nowych pojazdach osobowych oraz dostawczych do 3,5 tony, które uzyskały homologację, montowane są urządzenia systemu eCall.

KORZYŚĆ

System może przyczynić się do zmniejszenia liczby ofiar wypadków na drogach. Od października 2017 (gdy przystosowano do eCall Centrum Powiadamiania Ratunkowego) do końca 2017 roku w Polsce na numer alarmowy 112 skierowano 43 zgłoszenia eCall.

Poza automatyzacją transportu i C-ITS warto zwrócić uwagę na trendy takie jak mobilność jako usługa (zamiast posiadać własne środki transportu użytkownicy wynajmują dostępne środki w miarę potrzeby), mobilność współdzielona (użytkownicy współdzielą własny lub wynajęty środek transportu z innymi użytkownikami) oraz integracja transportu multimodalnego (planowanie rozwoju i korzystania z transportu w podejściu integrującym wszystkie dostępne środki transportu).

Rozwój polskiej infrastruktury szynowej, taboru, ich wzajemnej komunikacji i wymiany danych (w tym także zastosowań urządzeń IoT), stają się koniecznością w XXI wieku. Wyzwania z budową zintegrowanego systemu transportowego w kraju i interoperacyjności międzygałęziowej i międzynarodowej, a w perspektywie rozwiązania quasi-szynowe jak kolej magnetyczna, próżniowa czy obecnie już wprowadzane rozwiązania dwu i wielosystemowe (uniwersalizacja i interoperacjonalizacja transportu) wymagają określonych działań skoncentrowanych w identyfikowanym i sprawnym (nie rozproszonym funkcjonalnie) ośrodku badawczym, wdrożeniowym, a przede wszystkim ośrodku decyzyjnym. Głównymi efektami powinny być:

1. Podwyższone prędkości pojazdów szynowych, również w kontekście budowy sieci połączeń szybkich, w tym związanych z CPK (Centralny Port Komunikacyjny).
2. Racjonalizacja pracochłonności i kosztów utrzymania coraz bardziej złożonej infrastruktury.
3. Informatyzacja i automatyzacja procesów w transporcie kolejowym, zarówno wewnętrznych, jak i na styku z otoczeniem gospodarczym, celem efektywnego wpisania kolei w łańcuchy transportowe (multimodalizacja łańcuchów dostaw i podróży) oraz szeroko rozumiane cyberbezpieczeństwo.
4. Zapewnienie, poprzez udział podmiotów kolejowych w procesie badań i rozwoju, że nowe rozwiązania będą spełniały oczekiwania ich przyszłych użytkowników (UX – *user experience).*
5. Tworzenie warunków do rozwoju polskich rozwiązań innowacyjnych, inteligentnych specjalizacji rozwoju przemysłu 4.0 oraz eksportu o wyższej wartości dodanej.

W sektorze transportu szynowego (przede wszystkim – kolejowego) warunki rozwoju IoT są specyficzne, co wynika przede wszystkim z odmiennej filozofii organizacji przewozów. Pojazd „jest prowadzony" przez drogę (szynową), a różnice występują w odniesieniu do stopnia swobody określania prędkości i płynności poruszania się pojazdu po wcześniej zdefiniowanej trasie. Obrazowo ujmując: w transporcie drogowym występuje

„domyślne zielone" (ruch jest stanem domyślnie dozwolonym), a na kolei – „domyślne czerwone" (ruch jest dozwolony dopiero po uzyskaniu zezwolenia). Stawiane są też znacznie wyższe wymogi wstępne, a w zamian zapewnione jest większe bezpieczeństwo (zasada *fail-safe*).

Transport kolejowy obfituje w rozliczne urządzenia zabezpieczające prowadzenie ruchu, przy czym ich mnogość (rozpatrywana zwłaszcza przez pryzmat jednolitego rynku europejskiego) sama w sobie stanowi wyzwanie. Te same funkcje są realizowane w odmienny sposób na poszczególnych krajowych sieciach kolejowych, zaś wdrażanie interoperacyjności napotyka na bariery wynikające z różnic zastałych, stąd priorytet osiągnięcia pełnej interoperacyjności na głównych szlakach kolejowych, by nie obciążać nadmiernymi kosztami dostosowania całości infrastruktury.

Podstawowym ogniwem transmisji informacji w obszarze transportu kolejowego pozostaje człowiek, dlatego celem rozwoju IoT jest przede wszystkim automatyzacja. Najprostszym przykładem bezpośredniej komunikacji pomiędzy poszczególnymi elementami systemu kolejowego jest SSP (samoczynna sygnalizacja przejazdowa). Wskutek impulsu wywołanego ze strony pojazdu osiągającego określony punkt na linii kolejowej następuje samoczynne zamknięcie rogatek przejazdowych – bezpośrednia komunikacja pomiędzy układem pojazd-tor a urządzeniami SSP eliminuje stanowisko dróżnika przejazdowego. Równocześnie, dla większego zabezpieczenia, prawidłowe zamknięcie rogatek (prawidłowe zabezpieczenie przejazdu drogowo-kolejowego) jest sygnalizowane poprzez stosowny komunikat dopuszczający jazdę, wyświetlany na tarczy ostrzegawczej przejazdowej. W tym przypadku odbiorcą sygnału jest jednak nie pojazd, lecz człowiek (maszynista) i to jego obowiązkiem jest odpowiednia reakcja (zatrzymanie pociągu) w razie braku sygnału zezwalającego na tarczy sygnalizatora.

Nad prawidłowym funkcjonowaniem transportu kolejowego czuwa szereg czujników odpowiedzialnych za przekazywanie informacji o stanie danego urządzenia. Wyróżnić tu można wspomniane urządzenia detekcji pociągu w ramach SSP, urządzenia kontroli położenia iglic rozjazdowych, urządzenia kontroli zajętości toru, system SHP (samoczynnego hamowania pociągu), inicjujący zatrzymanie składu w razie braku sygnału aktywności ze strony maszynisty. Postęp w zakresie automatyki kolejowej najlepiej obrazują urządzenia DSAT (detekcji stanów awaryjnych w taborze), wychwytujące w przejeżdżającym pociągu usterkę, wskazując konkretny element nawet w 40-wagonowym składzie przejeżdżającym z prędkością kilkudziesięciu km/h. Rozwój oczujnikowania transportu kolejowego w połączeniu z rozwojem bezpośredniej komunikacji pomiędzy poszczególnymi urządzeniami może w istotny sposób zwiększyć poziom bezpieczeństwa, niezawodności i możliwości przewozowych na kolei.

Podobnie jest w sytuacji BSP (bezzałogowych statków powietrznych), gdzie oczujnikowanie umożliwia zbieranie i analizę danych, a w przyszłości usługi transportowe, pomiary jakości powietrza i wspieranie sieci teleinformatycznych, znajdą zastosowanie w różnych gałęziach gospodarki.

Obecny wzrost liczby pojazdów BSP następuje w wyniku dobrej koniunktury gospodarczej, rosnącej dostępności technologii, liberalnych regulacji i malejących kosztów BSP. W Polsce liczba operatorów dronów posiadających świadectwo kwalifikacji w styczniu 2019 roku przekroczyła dziesięć tysięcy. Przyszłości BSP upatruje się jednak w pojazdach automatycznych i autonomicznych.

GSA (European Global Navigation Satellite Systems Agency) na konferencji European Space Week w Marsylii w grudniu 2018 r. wskazała BSP jako nowego użytkownika systemów EGNOS oraz Galileo, czego dowodem są liczne projekty finansowane przez programy unijne (m.in. Horyzont 2020). Szczególne zainteresowanie budzą projekty: REAL (RPAS EGNOS Assisted Landings), w ramach którego naukowcy opracowują czujniki nawigacyjne oparte na EGNOS (European Geostationary Navigation Overlay Service) z wykorzystaniem m. in. integralności sygnału satelitarnego, oraz GAUSS (Group of Astrodynamics for the Use of Space Systems), którego celem jest m.in. zastosowanie systemu automatycznego dozorowania ADS-B (Automatic Dependent Surveillance-Broadcast) do pozycjonowania statków powietrznych.

Jednym z ważniejszych elementów w zakresie regulacji prawnych dotyczących użytkowania BSP jest ochrona prywatności i danych osobowych. Należy mieć na uwadze, że w trakcie użytkowania BSP będzie dochodziło również do przetwarzania danych osobowych. Rozważenia wymaga kwestia komu przypisać rolę administratora danych, jak również sposób realizacji jego obowiązków wynikających z przepisów o ochronie danych osobowych. Każdorazowo należy położyć szczególny nacisk na zapewnienie prywatności osób, których dane dotyczą, nie tylko w fazie projektowania, lecz również domyślnej ochrony danych w zakresie użytkowania BSP.

W lutym 2019 r. Ministerstwo Infrastruktury wraz z Polskim Instytutem Ekonomicznym opublikowały Białą Księgę Bezzałogowych Statków Powietrznych. Księga podsumowuje etap koncepcyjno-realizacyjny programu, którego elementem było m.in. opracowanie i wdrożenia rozporządzenia MI ułatwiającego loty BVLOS (Beyond Visual Line of Sight) i dopuszczającego loty automatyczne, jak również uruchomienie programu CEDD (Centralnoeuropejski Demonstrator Dronów) na obszarze Górnośląsko-Zagłębiowskiej Metropolii. Program CEDD jest działaniem pilotażowym, przygotowującym infrastrukturę dla lotów automatycznych i autonomicznych oraz założenia do dalszej fazy regulacji dla BSP.

Na szczeblu zarówno międzynarodowym, jak i europejskim, trwają prace nad regulacjami prawnymi użytkowania BSP, które nie obejmują jednak kwestii prywatnoprawnych. Dopóki takich regulacji nie ma, kluczowe są regulacje krajowe. Polska była jednym z pierwszych krajów, który stworzył regulacje dotyczące operacji VLOS (Visual Line of Sight) – w 2013 r., znowelizowane w 2016 r. W lutym 2019 r. weszło w życie rozporządzenie, które zezwala na operacje BVLOS. Prace mające na celu dostosowanie regulacji krajowych do rozporządzenia UE trwają obecnie w ramach projektu naukowego „Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym." finansowanego przez Narodowe Centrum Nauki (nr 2017/27/B/HS5/00008) – jest on realizowany na Wydziale Prawa i Administracji Uczelni Łazarskiego w Warszawie (strona projektu: https://prawodrony.pl).

W logistyce XX wieku duży przełom nastąpił dzięki standaryzacji sposobu przewożenia ładunków poprzez ich paletyzację i (zwłaszcza) konteneryzację. Podobny przełom w wieku XXI może (i powinien) nastąpić dzięki cyfryzacji i stopniowej, integrującej multimodalizacji transportu. Aby było to możliwe, niezbędna jest szersza koordynacja działań w tych obszarach. Niebagatelną rolę w rozwoju zintegrowanych multimodalnych łańcuchów dostaw, oprócz niezwykle ważnych zmian organizacyjnych i mentalnych, mają i będą miały rozwiązania techniczne, takie jak upowszechnienie i standaryzacja wymiany danych, co zostanie walnie wsparte przez Internet (w tym Internet Rzeczy) oraz cyfryzację procesów transportowo-logistycznych.

Kluczowym elementem łańcucha dostaw jest dokumentacja przewozowa. Jej przechowywanie i prawidłowość ma bezpośredni wpływ np. na możliwość zastosowania preferencyjnej stawki podatku VAT. Proces digitalizacji dokumentów przewozowych na pewno usprawni i umożliwi większą automatyzację procesów transportowo-logistycznych.

Digitalizacja dokumentów przewozowych postępuje przede wszystkim poprzez dwa międzynarodowe projekty: e-AWB (air waybill) dla transportu lotniczego oraz e-CMR (CMR = fr. *Convention relative au contrat de transport international de marchandises par route*) dla transportu drogowego.

IATA (International Air Transport Association) ogłosiła, że z dniem 1 stycznia 2019 roku, e-AWB staje się domyślną postacią umowy przewozu w transporcie lotniczym towarów. Wówczas odsetek elektronicznych listów przewozowych na całym świecie przekroczył 60%, w Europie – 50%. W Polsce wskaźnik ten wyniósł 26,5%, przy dynamicznym wzroście (z poziomu 9,5% rok wcześniej).

Wciąż jednak część przewoźników cargo w Polsce nie umożliwia transmisji danych e-AWB (co powinno ulec poprawie w tym roku). Ograniczenia dotyczą również różnych destynacji na świecie, ze względu na uwarunkowania lokalne w krajach docelowych. Całkowita rezygnacja z papierowych listów lotniczych nie jest jeszcze w Polsce możliwa. Nawet w przypadku zastosowania e-AWB, z praktycznego punktu widzenia, i tak papierowy wydruk tego dokumentu jest zazwyczaj niezbędny na potrzeby operatorów cargo w portach lotniczych (najczęściej są to spółki Skarbu Państwa), a także administracji celno-skarbowej.

Za przykład modelowy uznać można terminale kontenerowe portu morskiego w Gdyni, gdzie integracja systemów, w tym cyfrowa transmisja danych pomiędzy spedytorem, armatorem, operatorem terminala kontenerowego oraz służbą celno-skarbową, eliminuje konieczność korzystania z papierowych listów przewozowych do absolutnego minimum (najczęściej tylko na życzenie eksportera). Lotniska w Polsce mają jeszcze sporo do nadrobienia.

Elektroniczny list przewozowy w transporcie drogowym e-CMR znajduje się wciąż w fazie przygotowań i testów. Pierwszy testowy transport z użyciem e-CMR odbył się dopiero dwa lata temu, na trasie z Hiszpanii do Francji. Praktyczne zastosowanie e-CMR przyniesie dużo korzyści dla wszystkich zainteresowanych stron. Nadawcy i odbiorcy otrzymają większe niż do tej pory możliwości zdalnego nadzoru (śledzenia) przesyłek, możliwość większej integracji systemów zlecania wysyłek, potwierdzania dostaw (np. dla wewnątrzwspólnotowego nabycia towarów), na obiegu dokumentów księgowych i przepływach finansowych kończąc. Służby państwowe otrzymają zwiększone możliwości kontroli przewozów w czasie rzeczywistym, co powinno pozytywnie wpłynąć na uszczelnianie systemów podatkowych. Integracja e-CMR z systemem e-Call stosowanym w pojazdach przełoży się z kolei na poprawę bezpieczeństwa na drogach (przykład: pojazd przewożący towary niebezpieczne uległ wypadkowi, system e-Call automatycznie powiadamia o zdarzeniu odpowiednie służby, a dane z e-CMR pozwolą w czasie rzeczywistym zidentyfikować skalę zagrożenia). Z kolei dla przewoźników i spedytorów e-CMR umożliwi m.in. efektywniejszą administrację dokumentami i procesami księgowymi. Obecnie w transporcie drogowym w Europie termin płatności za wykonaną usługę transportową liczony jest najczęściej od daty wpływu do siedziby płatnika papierowego (!) oryginału dokumentu przewozowego CMR. Zastąpienie papierowego listu przewozowego dokumentem elektronicznym powinno skrócić przepływy finansowe od około dwóch do sześciu tygodni, co znacznie zmniejszy koszty obrotu i uwolni obecnie zamrożony w procesach rozliczeniowych kapitał.

Kluczowym elementem e-CMR jest powstały w 2008 roku dodatkowy protokół do konwencji CMR. Do tej pory podpisały go: Bułgaria, Czechy, Dania, Estonia, Finlandia, Francja, Hiszpania, Holandia, Iran, Litwa, Luksemburg, Łotwa, Mołdawia, Rosja, Słowacja, Słowenia, Szwajcaria oraz Turcja. Polska jest stroną konwencji CMR, niemniej jednak dotąd nie podpisała dodatkowego protokołu dotyczącego e-CMR. Prace w tym zakresie trwają.

SAFETY PILOT – TESTY SYSTEMU OSTRZEGANIA PRZED WYPADKAMI

HTTP://SAFETYPILOT.UMTRI.UMICH.EDU
ANN ARBOR, MICHIGAN, USA

PROBLEM

Duża liczba karamboli drogowych i korków powstających w związku z wypadkami.

ROZWIĄZANIE

W roku 2012 Dziennik Internautów opisywał testy rozwiązania Safety Pilot, które łączyło w sobie ideę V2I oraz V2V.
W ramach testów prowadzonych w mieście Ann Arbor w stanie Michigan w 3 tys. aut zamontowano urządzenia, które rejestrowały informacje o prędkości i położeniu pojazdów oraz przesyłały je do innych aut na drodze. Dzięki temu kierowca mógł być ostrzeżony przed możliwym wypadkiem.

KORZYŚĆ

Zdaniem Krajowej Agencji Bezpieczeństwa Ruchu Drogowego (NHTSA) udało się udowodnić, że rozwinięte już technologie naprawdę działają i z reguły są akceptowane przez kierowców.

Według szacunków, udział polskich przewoźników w całym europejskim rynku przekroczył 30%, stawiając nas na pozycji lidera. Powinniśmy zatem jako kraj być tym bardziej zainteresowani wdrożeniem e-CMR. Tymczasem cyfryzacja dokumentów przewozowych w transporcie drogowym w Polsce polega głównie na digitalizacji papierowych wersji po wykonaniu usługi (sic!). To rozwiązanie nie jest oczywiście optymalne, szczególnie wobec korzyści, jakie może wygenerować stosowanie e-CMR w całym łańcuchu dostaw.

W sytuacji niedoboru uregulowań odgórnych tworzone są inicjatywy oddolne jak np. globalne standardy identyfikacyjne i komunikacyjne GS1 jako kluczowy czynnik umożliwiający funkcjonowanie koncepcji IoT. GS1 to globalny system standardów i rozwiązań biznesowych tworzonych od 1973 r. z inicjatywy i pod przewodnictwem grupy przedsiębiorstw. Standardy GS1 stanowią uzgodnione zasady i wytyczne, które w jednolity sposób są stosowane przez podmioty w wielu branżach w celu usprawnienia operacji w łańcuchach dostaw.

Globalne standardy GS1 umożliwiają wykorzystywanie jednoznacznych kluczy do identyfikacji dóbr, usług, zasobów, lokalizacji itp. na całym świecie. Klucze te mogą być przedstawione w nośnikach danych, jak kody kreskowe lub znaczniki EPC/RFID (Electronic Product Code / Radio-Frequency Identification), co umożliwia ich automatyczny odczyt. Mogą być również wykorzystywane w komunikacji elektronicznej, wpływając na poprawę szybkości i dokładności przesyłanych danych podstawowych, danych transakcyjnych, jak również danych o zdarzeniach zachodzących na bieżąco w łańcuchu dostaw. Duże ilości zebranych danych mogą być przechwytywane, przechowywane, analizowane, kierowane, wyszukiwane, współdzielone, znacznie wykraczając poza możliwości tradycyjnych relacyjnych systemów baz danych. Obecnie jakość danych jest ważniejsza niż kiedykolwiek wcześniej, a standardy GS1 stanowią podstawę wiarygodnych, możliwych do udostępniania, przeszukiwania i łączenia danych, począwszy od danych podstawowych po rozszerzone atrybuty związane z identyfikacją poszczególnych obiektów w łańcuchu dostaw.

Współdzielenie informacji jako filar GS1 dotyczy czterech obszarów:

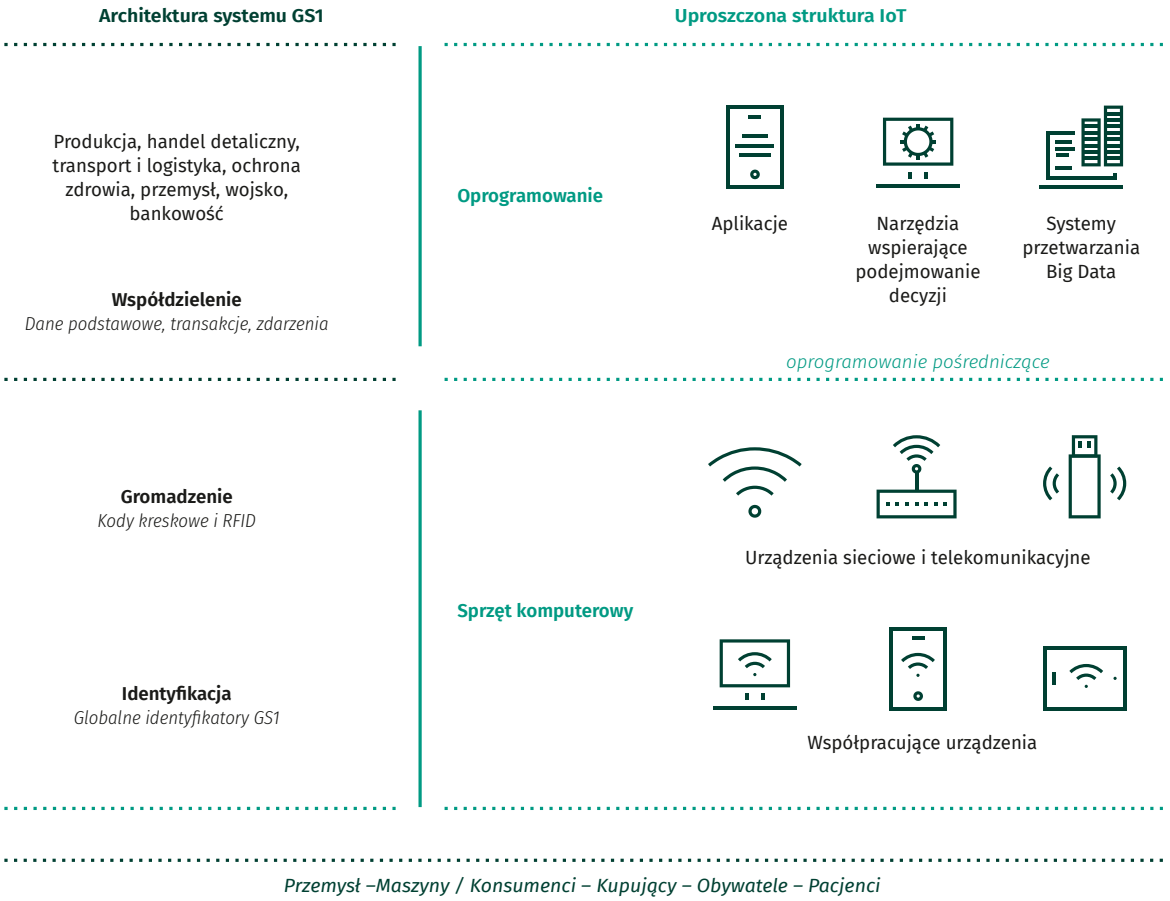
- GS1 EDI (elektronicznych dokumentów biznesowych),
- GDSN (podstawowych danych o produktach),
- EPCIS (informacji o zdarzeniach dotyczących przepływu towarów w łańcuchu dostaw),
- opisu informacji o produkcie w Internecie.

Budowanie otwartych rejestrów, platform czy standardowych połączeń komunikacyjnych służących wymianie zgromadzonych danych to zasadnicza część działalności organizacji GS1. Aspekt ten jest również niezwykle istotny w koncepcji IoT odnoszącej się do warstwy aplikacji, której podstawowymi funkcjami poza zapewnieniem bezpieczeństwa danych jest ich przechowywanie i analiza.

Współdzielenie informacji jako filar GS1 dotyczy czterech obszarów: elektronicznych dokumentów biznesowych (GS1 EDI), podstawowych danych o produktach (GDSN), informacji o zdarzeniach dotyczących przepływu towarów w łańcuchu dostaw (EPCIS) oraz opisu informacji o produkcie w Internecie. Budowanie otwartych rejestrów, platform czy standardowych połączeń komunikacyjnych służących wymianie zgromadzonych danych to zasadnicza część działalności organizacji GS1. Aspekt ten jest również niezwykle istotny w koncepcji IoT odnoszącej się do warstwy aplikacji, której podstawowymi funkcjami poza zapewnieniem bezpieczeństwa danych jest ich przechowywanie i analiza. Kluczowe elementy IoT to również połączone urządzenia, które mogą obejmować zarówno czytniki kodów kreskowych, znaczniki RFID, jak i czujniki. Działają one na zasadzie interfejsów między jednoznacznie zidentyfikowanymi obiektami a kolejnymi warstwami architektury IoT. Dane w nich są przesyłane, przechowywane i analizowane.

Koncepcja IoT obiecuje daleko idące korzyści również z perspektywy branży TSL (Transportu–Spedycji–Logistyki), w szczególności dla operatorów logistycznych, ich klientów biznesowych, a także konsumentów końcowych. Korzyści te obejmują cały łańcuch wartości logistycznych, począwszy od procesów zaopatrzenia, produkcji, operacji magazynowych, transportu czy dystrybucji do klienta końcowego. IoT, poprzez monitorowanie stanu zasobów, przesyłek, jednostek logistycznych, czy osób w czasie rzeczywistym, umożliwia pełną przejrzystość w całym łańcuchu dostaw. Internet Rzeczy może zoptymalizować sposób, w jaki ludzie, systemy i zasoby współpracują ze sobą przy równoczesnej koordynacji tych działań. Standaryzacja w tym zakresie ma na celu podniesienie efektywności procesów biznesowych i zapewnienie oszczędności poprzez automatyzację opartą na globalnie unikalnej identyfikacji obiektów oraz standaryzacji sposobu komunikacji w globalnych łańcuchach dostaw.

Standardy GS1 w koncepcji IoT



Źródło: GS1 Polska.

Transport kosmiczny cechuje się daleko odmiennymi warunkami użytkowania. Do samego jego istnienia niezbędna jest wyspecjalizowana infrastruktura wynosząca. Przełamanie bariery grawitacji ziemskiej i wyniesienie statku kosmicznego w przestrzeń kosmiczną wymaga bardzo wysokich prędkości (pierwsza i druga prędkość kosmiczna), a tym samym wyposażenia pojazdu w napęd o znacznej mocy i zużywający dużo energii. Tego typu transport wymaga wyjątkowo precyzyjnych urządzeń nadzoru i pomiaru, w tym z zakresu Internetu Rzeczy, oraz znacznego stopnia automatyzacji. Wynika to z kosztów wysokonakładowego czynnika ludzkiego (w tym załogi pojazdu), którego użycie wiąże się ze znacznymi niedogodnościami i ryzykami, a tym samym kosztami (brak grawitacji i dostępu do zasobów naturalnych, promieniowanie jonizujące). Znaczny udział we flocie pojazdów kosmicznych stanowią pojazdy bezzałogowe (w tym satelity) o różnym, zazwyczaj dużym stopniu automatyzacji.

Misja kapsuły Crew Dragon to bezzałogowy test systemu, który w niedalekiej przyszłości posłuży wynoszeniu astronautów do Międzynarodowej Stacji Kosmicznej (ISS) i sprowadzaniu ich z powrotem na Ziemię. Od końca ery wahadłowców amerykański program załogowy i loty wymiany załóg ISS są zależne od rosyjskiego systemu Sojuz. NASA chce zakończyć tą zależność komercyjnymi kontraktami na wynoszenie załóg, które wygrały firmy SpaceX i Boeing.

Statek Crew Dragon firmy SpaceX wystartował 2 marca o 8:49 czasu polskiego na rakiecie Falcon 9 w pierwszym locie demonstracyjnym do Międzynarodowej Stacji Kosmicznej. W dniu 3 marca, kapsuła załogowa Crew Dragon wykonała udaną operację zbliżenia i dokowania do Międzynarodowej Stacji Kosmicznej. Statek został automatycznie przytwierdzony do portu IDA przy module Harmony, a astronauci rezydujący na stacji weszli na jego pokład. Statek przeprowadził przed dokowaniem kilka manewrów demonstracyjnych w pobliżu stacji, pokazujących gotowość jego systemów do przyszłych operacji z ludźmi na pokładzie. W trakcie lotu odłączono dolną część rakiety, która wylądowała autonomicznie na barce. Warto odnotować, że w pracach nad algorytmami nawigacji i naprowadzenia pracował przez kilka lat polski programista, Tomasz Czajka, absolwent Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Był to pierwszy lot amerykańskiej kapsuły załogowej od czasu zakończenia programu wahadłowców w 2011 roku.

Loty kosmiczne to nie tylko loty na Międzynarodową Stację Kosmiczną, ale również komercyjne loty pasażerskie. Turystyka lotnicza istnieje i rozwija się z roku na rok. Szacuje się, że przed 2030 r. realne jest osiągnięcie poziomu pięciu milionów pasażerów kosmicznych rocznie. Wizja ta zakłada stworzenie wyrafinowanej infrastruktury turystyki kosmicznej z łącznie ponad stu orbitalnymi hotelami i centrami sportowymi, a także codziennym rozkładem lotów księżycowych i stworzeniem hoteli biegunowych. Obecnie istnieją dwie możliwości wykonywania lotów suborbitalnych. Pierwsza wzorowana jest na statku kosmicznym SpaceShipOne, czyli używa się samolotu, który wynosi właściwy statek kosmiczny na wysokość kilkunastu kilometrów, gdzie odłącza się i uruchamia własny napęd rakietowy, już samodzielnie wznosząc się wyżej. Powrót może nastąpić w dwojaki sposób: albo statek kosmiczny wraca do miejsca, skąd został oderwany albo wraca do innego miejsca na Ziemi (jest to tzw. „transport kosmiczny"). Druga opcja, jest wzorowana na „Delta Clipper Experimental", używa rakiety z kapsułą na górze, następnie kapsuła oddziela się od rakiety na pewnej wysokości. Obie części wracają na ziemię niezależnie od siebie.

W związku z turystyką kosmiczną powstanie potrzeba stworzenia regulacji w zakresie odpowiedzialności za szkody spowodowane takim turystom. Obecnie obowiązujące konwencje uchwalone kilkadziesiąt lat temu nie tylko nie uwzględniały takich możliwości, ale cedują również odpowiedzialność wyłącznie na państwa, co w przypadku lotów komercyjnych nie wydaje się właściwym rozwiązaniem.

Warto odnotować, że w Polsce znajduje się Baza Badawcza Lunares (jedyny tego typu obiekt w Europie), w której przy pomocy sensorów IoT prowadzone są badania z zakresu psychologii czynników ludzkich podczas załogowych lotów kosmicznych oraz testy nowoczesnych technologii, nie tylko z sektora kosmicznego. Placówka jest całkowicie odizolowana od środowiska zewnętrznego, wliczając 250 metrów kwadratowych powierzchni spacerów kosmicznych. Infrastruktura Bazy pozwala na ciągłe monitorowanie zdrowia, zachowań mieszkańców oraz pełną immersję podczas symulowanych misji załogowych. Baza Lunares (zwana również Habitatem) to obiekt unikatowy, z którego wymierne korzyści odnoszą zarówno podmioty naukowe, jak i świat biznesu. Przykładem wykorzystania Habitatu są badania prowadzone przez naukowców z Wydziału Matematyki, Informatyki i Mechaniki UW. Analogowi astronauci byli odcięci od zewnętrznego świata, naturalnego światła czy zewnętrznych dźwięków. Komunikacja z kontrolą misji była opóźniona, a sami astronauci podążali za dostosowanym czasem marsjańskim. Celem takich symulacji jest poznanie potencjalnych problemów mogących wystąpić podczas faktycznych misji kosmicznych. Do tej pory zachowanie załogi nie było jednak mierzone narzędziami socjometrycznymi pozwalającymi na dużą dokładność. Dodatkowym czynnikiem wyróżniającym przedstawianą misję była symulacja wypadków – wpływu niepełnosprawności i śmierci na powodzenie misji.

Zakres możliwego wykorzystania IoT

Poza usługami dnia 1 i dnia 1.5 wymienionymi w Tabeli 1 możliwe są również inne zastosowania IoT w transporcie:

- optymalizacja zużycia energii elektrycznej w pojazdach autonomicznych – rozwój systemu odzyskiwania energii kinetycznej typu KERS (Kinetic Energy Recovery System) na bazie czujników położenia oraz doboru trasy o najniższym „oporze";
- predykcja ruchu drogowego: czasów przejazdu i natężeń ruchu;
- systemy zarządzania ruchem – zbieranie danych o położeniach, prędkościach i trasach pojazdów celem lepszego zarządzania ruchem, np. sterowaniem światłami w ruchu drogowym, proponowanie bezpiecznych i szybkich tras dla różnych środków transportu, np. dla dronów lub dla transportu szynowego;
- identyfikacja wypadku lub kolizji i automatyczne powiadamianie służb ratunkowych (eCall);
- zbieranie danych o poziomie wody, oblodzeniu (transport wodny);
- monitorowanie statków, tworzenie mapy położeń statków;
- lokalizowanie pojazdów, poprawa przepustowości sieci poprzez zmniejszanie odstępu między pojazdami (w razie potrzeby i możliwości), sterowanie prędkością ich jazdy;
- nadzór nad eksploatacją i utrzymaniem urządzeń infrastrukturalnych;
- optymalizacja wykorzystania poszczególnych elementów infrastruktury transportowej, optymalizacja tras, optymalizacja pracy całości systemu;
- optymalizacja eksploatacji pojazdów transportu publicznego;
- nadawanie priorytetów dla komunikacji zbiorowej;
- detekcja wykroczeń (np. weryfikacja prędkości, nieuprawnionego wjazdu do strefy czystego transportu);
- monitorowanie przesyłek w logistyce, np. warunków przewozu ładunków specjalnych lub wrażliwych (np. leków, żywności, materiałów niebezpiecznych, ładunków ponadnormatywnych).

Bariery

W toku prac Grupa zidentyfikowała następujące bariery dla branży:

1. Duża złożoność procesów transportowo-logistycznych.
2. Planowanie i zarządzanie transportem w skali mikro (niezależne dla różnych środków transportu, różnych jednostek przestrzennych i różnych zarządców transportu), brak makroskopowego, holistycznego planowania.
3. Zamykanie się podsystemów transportowych i logistycznych we własnych ramach, bez udostępniania danych na zewnątrz. Niejasne perspektywy implementacji Dyrektywy 2010/40/UE z dnia 7 lipca 2010 r. (w sprawie ram wdrażania inteligentnych systemów transportu) w krajach członkowskich, w tym w Polsce.
4. Niewystarczająca wymiana informacji między zarządcami infrastruktury, operatorami i użytkownikami (licencjonowanie, systemy zamknięte, interfejsy autorskie), np. brak interoperacyjności między systemami TMS, WMS i GPS, brak wymiany informacji o wypadkach i utrudnieniach w ruchu między zarządcami infrastruktury.
5. Brak normalizacji (standaryzacji) procesów i narzędzi lub niski stopień ich upowszechnienia powoduje, że firmy tworzą własne rozwiązania i procesy, pozbawione waloru interoperacyjności. Przykładem jest archaiczny proces transmisji danych w przypadku zleceń transportowych, gdzie wg szacunków 90% zleceń jest przesyłanych mailowo w formacie pdf a 10% w plikach tekstowych. Brak standaryzacji powoduje nieopłacalność tworzenia przystępnych cenowo programów do zarządzania procesami, upowszechniających współczesne możliwości komunikacji i wymiany danych zgodne z oczekiwaniami firm transportowo-logistycznych, szczególnie małych i średnich.
6. Brak obowiązku prawnego posiadania urządzeń do geolokalizacji – w praktyce posiadanie takich urządzeń jest normą w przypadku pojazdów ciężkich, ale w transporcie lekkim do 3,5 t współczynnik zainstalowanych geolokalizatorów w samochodach jest znacznie mniejszy.
7. Brak jednolitych standardów w urządzeniach do geolokalizacji.
8. Niewystarczające regulacje prawne dla pojazdów komunikujących się między sobą (V2V) i z infrastrukturą (V2I), a także pojazdów autonomicznych, pomimo zaawansowanych prac technicznych nad tymi rozwiązaniami.

PROJEKT SCOOP@F – BADANIE INTEROPERACYJNOŚCI WIELU USŁUG C-ITS

HTTP://WWW.SCOOP.DEVELOPPEMENT-DURABLE.GOUV.FR/EN/
FRANCJA

PROBLEM

Brak zweryfikowanej interoperacyjności różnych usług C-ITS, szczególnie w dużej skali.

ROZWIĄZANIE

Celem projektu było wsparcie wdrożenia podstawowych usług C-ITS na poziomie krajowym poprzez testy na dużą skalę współpracy wielu takich usług. Miało to pozwolić na weryfikację w warunkach rzeczywistych takiego wdrożenia i interoperacyjności różnych rozwiązań technicznych i usług. SCOOP@F był projektem przedwdrożeniowym dla różnych technologii C-ITS we Francji, zrealizowanym po pomyślnym zakończeniu w lipcu 2013 r. projektu testów terenowych SCORE@F. Projekt angażował przemysł i administrację drogową, kluczowymi partnerami były Renault i PSA, które poszukiwały modelu biznesowego dla wszystkich interesariuszy.

KORZYŚĆ

Przetestowano w warunkach rzeczywistych w dużej skali współpracę wielu usług C-ITS, co będzie miało kluczowe znaczenie dla przyszłego wdrażania takich usług.

9. Niedobór instalacji infrastruktury C-ITS oraz ograniczenia w zakresie niezawodnej i wydajnej transmisji danych w kierunku do infrastruktury, jak i między pojazdami (V2V).

10. Wykorzystywanie dedykowanych dla technologii ITS częstotliwości przez podmioty, które uzyskały zgody na nadawanie w tym paśmie jeszcze przed wprowadzeniem zarządzenia Prezesa UKE (Zarządzenie Nr 56 Prezesa Urzędu Komunikacji Elektronicznej z dnia 15 października 2009 r. zmieniające zarządzenie w sprawie planu zagospodarowania częstotliwości dla zakresu 5875-5925 MHz) lub nadające nielegalnie.

11. Niewystarczające możliwości realnego tworzenia stref czystego transportu pomimo problemu zanieczyszczenia powietrza w polskich miastach.

12. Brak prawnych możliwości dla zarządców dróg w miastach do wykorzystania systemów automatycznego wykrywania niektórych naruszeń.

13. Obecnie karta SIM wykorzystywana do przesyłania danych w systemu eCall jest „uśpiona", tzn. aktywuje się tylko po wypadku, nie można więc wykorzystać systemu np. do odnajdywania skradzionego samochodu lub do monitorowania położeń pojazdów na potrzeby predykcji ruchu lub systemów zarządzania ruchem (pojazdy autonomiczne mogą być coraz częściej wypożyczane na krótko, a nie posiadane, dlatego zmniejszą się obawy związane z potencjalną identyfikacją użytkowników, więc informacje o położeniach pojazdów można będzie zbierać na bieżąco). eCall jest podsystemem zamkniętym, producenckim, który ze względu na status podsystemu krytycznego nie umożliwia dostępu do swoich zasobów (interfejsu sieciowego) w celu realizacji innych usług typu augmented/value-added/enhanced services.

14. Wyzwaniem jest uregulowanie kwestii związanych z użytkowaniem BSP do nagrywania obrazu, postrzeganego jako największe zagrożenie dla prywatności obywateli.

15. Bariera wprowadzania automatyzacji w małych i średnich przedsiębiorstwach. W firmach transportowych częstą przyczyną braku automatyzacji procesów przy pomocy IoT jest różnica pokoleniowa. Znaczna część właścicieli firm ma opory przed wdrażaniem nowych rozwiązań IT, gdyż nie do końca rozumie i widzi potrzebę zmian i korzyści, jakie z niej płyną. Częstym problemem jest również przyzwyczajenie do starych rozwiązań i strach przed nowymi systemami.

Propozycje działań rządu

Rekomendujemy następujące działania:

1. Stworzenie ram prawnych do makroskopowego zarządzania transportem, szczególnie w obszarach metropolitalnych i aglomeracjach miast, celem eliminacji narastających problemów zarządzania mikroskopowego. Wprowadzenie do porządku prawnego, np. Strategii Zrównoważonego Rozwoju Transportu 2030, ustawy „metropolitalnej" (aglomeracyjnej), ustaw „samorządowych", ustawy o drogach publicznych, ustawy o transporcie kolejowym, ustawy o publicznym transporcie zbiorowym, i wykonanie (pilotażowych) zintegrowanych studiów multimodalnych (ZSM), kierunkowych (określających kierunki rozwoju sieci i systemów transportowych) oraz szczegółowych (posiadających walor planistyczny), w obszarach metropolitalnych i aglomeracjach, ze szczególnym uwzględnieniem węzłów multimodalnych sieci TEN-T. W ramach zintegrowanych studiów multimodalnych na poziomie szczegółowym (planistycznym) możliwe byłoby określanie stref czystego transportu i stref rozwoju transportu autonomicznego.

2. Zapoznanie się z pracami grupy Profesora Tadeusza Zipsera na Politechnice Wrocławskiej, rozwijającej program do symulacji transportowych. W planach grupy jest także udostępnienie programu Orion – modelu symulacyjno-decyzyjnego, który ma za zadanie wymodelowanie decyzji planistycznych uwzględniających kompromis pomiędzy przebiegiem spontanicznych zjawisk w przestrzeni a regułami, które według przyjętej doktryny planistycznej mają być zrealizowane.

3. Standaryzacja wymiany i udostępniania danych między:
    - różnymi zarządcami infrastruktury,
    - zarządcami infrastruktury a operatorami/przewoźnikami,
    - zarządcami infrastruktury a użytkownikami końcowymi,
    - różnymi pojazdami (komunikacja V2V),
    - pojazdami i infrastrukturą (V2I),
    - systemami geolokalizacji (np. GPS), zarządzania flotą (TMS) i logistyką magazynową (WMS).

4. Regulacje dotyczące ochrony danych: pojazdy (np. samochody lub drony) skanują otoczenie i zbierają na jego temat dużo informacji, sporo danych może być też wymienianych pomiędzy pojazdami oraz z infrastrukturą – należy te dane zabezpieczyć – przy rosnącej dostępności danych nieosobowych powinna być wzmocniona ochrona danych osobowych

5. Stworzenie dokładniejszych regulacji dla pojazdów autonomicznych (ustawa o elektromobilności nie jest wystarczająca):
    - Definicja pojazdu autonomicznego.
    - Warunki dopuszczenie pojazdów autonomicznych do testów (a następnie do ruchu), w tym:
        - ubezpieczenie prac badawczych / ubezpieczenie pojazdów w rzeczywistym ruchu,
        - określenie odpowiedzialności za wypadek oraz procedur postępowania po wypadku,
        - ochrona niezmotoryzowanych użytkowników przestrzeni współdzielonej,
    - Instalacja czujników / urządzeń do komunikacji V2X w pojazdach.

6. Umożliwienie samorządom tworzenia realnych stref czystego transportu (SCT) i realnego zarządzania dostępem do nich. Konieczne jest wprowadzenie zmian w regulacjach, aby możliwe było wykorzystanie systemów IT na potrzeby SCT także w uzdrowiskach, miejscowościach turystycznych i miastach poniżej 100 tys. mieszkańców.

7. Umożliwienie automatycznej rejestracji naruszeń (np. nieuprawnionego wjazdu do stref czystego transportu). Obecnie miasta mogące tworzyć SCT nie posiadają dostatecznych możliwości egzekwowania prawa w przypadku stworzenia SCT.

8. Wprowadzenie obowiązku posiadania urządzeń do geolokalizacji w transporcie towarów.

9. Przygotowanie infrastruktury technicznej do przesyłania, przechowywania i przetwarzania dużej ilości danych pochodzących z pojazdów wyposażonych w urządzenia do komunikacji V2I. W szczególności: zbudowanie infrastruktury urządzeń C-ITS umożliwiających zbieranie danych ze wszystkich rodzajów pojazdów, przygotowanie baz danych oraz instalacja czujników i systemów przesyłu danych zbierających informacje o położeniach i prędkościach pojazdów oraz o usługach dodatkowych infrastruktury transportu, np. o wolnych miejscach postojowych.

10. Wyeliminowanie urządzeń, które mogą powodować zakłócenia w zakresie widma częstotliwości dedykowanych dla inteligentnych systemów transportowych, w pierwszej kolejności: dla pasma dedykowanego dla przypadków użycia związanych z bezpieczeństwem (Decyzja Komisji nr 2008/671/WE z dnia 5 sierpnia 2008r.).

11. Utworzenie Kolejowego Parku Naukowo-Technologicznego (KPN-T) wspierającego rozwój

innowacji oraz współpracę i koordynację działań (np. w obszarze B+R) pomiędzy producentami wyrobów i dostawców usług a podmiotami kolejowymi.

12. Wprowadzenie wymogu automatycznego przesyłania danych istotnych z punktu widzenia procesów transportowo-logistycznych (np. zmiana statusu ładunku lub pojazdu) zebranych offline w momencie pojawienia się w obszarze dostępu do Internetu.

13. Utworzenie ośrodka badawczo-wdrożeniowego i ośrodka decyzyjnego (nierozproszonych funkcjonalnie) w obszarze transportu.

14. Opracowanie (np. w ramach MI we współpracy z MC oraz MPiT) Białej Księgi Automatyzacji Transportu (BKAT). Biała Księga powinna: opisywać projekty i programy krajowe związane z automatyzacją transportu, zbierać doświadczenia w zakresie projektów pilotażowych z podziałem na środki i rodzaje transportu, oceniać skutki dotychczasowych działań. Powinna zostać wyszczególniona warstwa infrastrukturalna oraz pojazdy, należy też wziąć pod uwagę możliwości komunikacji pojazdów między sobą (V2V) oraz z infrastrukturą (V2I). Należy ocenić potencjał produkcyjny w Polsce i możliwość tworzenia łańcuchów wartości w zakresie automatyzacji. BKAT powinna zawierać propozycję wizji, celów głównych i szczegółowych oraz rekomendacje działań organizacyjnych, regulacji oraz finansowania działań. BK powinna uruchamiać konsultacje w celu opracowania założeń do przyszłej strategii automatyzacji transportu.

15. Stworzenie i popularyzacja programów kształcenia w zakresie nowoczesnych technologii zgodnych z wyzwaniami XXI wieku, w tym Internetu Rzeczy i Przemysłu 4.0, np. technik pojazdów autonomicznych (kierownik floty pojazdów autonomicznych itp.), technik transportu kosmicznego, kierownik floty pojazdów kosmicznych, kierownik turystyki kosmicznej, technik medycyny kosmicznej.

16. Stworzenie centrum kompetencji odpowiadającego za rozwój, testowanie i dopuszczanie do eksploatacji technologii autonomicznych. Tworzenie takiego centrum powinno przebiegać dwuetapowo.

    - Integracja działań ośrodków posiadających kompetencje w zakresie rozwoju i testowania pojazdów autonomicznych, z uwzględnieniem wszystkich aspektów koniecznych do dopuszczenia i wdrożenia pojazdów autonomicznych do operacyjnego zastosowania. Integracji ośrodków powinna towarzyszyć integracja poligonów i obszarów testowych, jak również opracowanie standardu dopuszczania terenu na potrzeby testów pojazdów (technologii) autonomicznych. Powinny zostać opracowane wytyczne prowadzenia testów koniecznych do uzyskania określonych uprawnień (np. wyjście z poligonu na obszar testowy, przejście z obszaru testowego na obszar miejski). Powinien zostać opracowany plan rozwoju technologii autonomicznych, któremu należy dedykować instrumenty finansowe (np. w ramach NCBR).

    - Wprowadzanie pilotażowych pasów/stref ruchu uspokojonego pojazdów autonomicznych przy większych inwestycjach towarzyszących, np. przebudowa linii średnicowej w Warszawie).

    - Ukonstytuowanie jednego ośrodka decyzyjnego lub ośrodka koordynującego w/w działania, uregulowanego ustawowo, z zapewnieniem odpowiedniego poziomu finansowania.

17

KIERUNKI DALSZYCH DZIAŁAŃ

Grupa Robocza dostrzega wyraźną potrzebę kontynuowania prac i wspólnego działania w dwóch obszarach – zaproszenie właściwych resortów do szczegółowej analizy postulowanych zmian prawnych oraz przygotowania praktycznych projektów badawczo-rozwojowych. Poniżej zaprezentowano robocze propozycje grupy.

Postulowane zmiany prawne

Jedną z ważniejszych barier rozwoju IoT, którą zidentyfikowały praktycznie wszystkie podgrupy branżowe, jest niedostosowanie systemu prawa do wyzwań nowoczesnych technologii. W trakcie prac sformułowano wstępnie kilkadziesiąt postulatów, które można przypisać następującym obszarom prawa:

Prawo telekomunikacyjne:

- dostosowanie przepisów prawnych do charakterystyki komunikacji M2M,
- podniesienie norm dopuszczalnego natężenia pola elektromagnetycznego,
- wprowadzenie definicji: komunikacji M2M, urządzenia końcowego przeznaczonego dla M2M,
- umożliwienie elastycznego podejścia w zakresie adresacji urządzeń M2M,
- dostosowanie czasu obowiązywania umowy pomiędzy konsumentem a dostawcą do długości życia produktu,
- wprowadzenie możliwości wykorzystywania danych biometrycznych przy rejestracji i autoryzacji użytkownika wykorzystującego usługi telekomunikacyjne,
- zniesienie obowiązku umieszczania numerów urządzeń M2M w usłudze biuro numerów i spis abonentów,
- umożliwienie bezprzewodowej zmiany operatora z wykorzystaniem standardu eSIM w przypadku komunikacji M2M,
- wyłączenie możliwości wykonywania połączeń na numery alarmowe w komunikacji M2M, za wyjątkiem urządzeń IoT, które wykorzystywane są w celach ratunkowych,
- wyłączenie komunikacji M2M z obowiązku cyklicznego udostępniania szczegółowych wykazów połączeń,
- zniesienie obowiązku numeracji urządzeń M2M w PNK, a także wprowadznie niższych opłat za numerację urządzeń M2M, jeżeli zostanie zastosowana,
- rozszerzenie uprawnień Prezesa UKE o przesłankę podjęcia działań, w sytuacji gdy występuje zagrożenie dla interoperacyjności interfejsów komunikacji wykorzystywanych do przesyłania danych z urządzeń końcowych M2M,

- rozszerzenie kompetencji Prezesa UKE w zakresie możliwości blokowania/ograniczania sprzedaży urządzeń końcowych M2M stwarzających ryzyko dla sieci, z uwagi na niespełnianie standardów telekomunikacyjnych,

- zapewnienie możliwości przetwarzania metadanych pochodzących z komunikacji M2M/IoT dla celów analitycznych, bez wymagania zgody użytkownika, przy zachowaniu warunków ochrony prywatności użytkowników.

Prawo zamówień publicznych:

- wprowadzenie zapisów zmuszających do doceniania rozwiązań opartych na zaawansowanych technologiach, np. wskazanych w krajowych inteligentnych specjalizacjach,

- wprowadzenie predefinicji procesu dialogu technicznego oraz partnerstwa innowacyjnego wspieranego przez instrumenty *„soft law"* (np. wytyczne, standardy) ułatwiające zastosowanie wspomnianego trybu partnerstwa innowacyjnego w praktyce,

- rozszerzenie katalogu sytuacji, w których wykorzystane mogą być spółki celowe,

- promowanie otwartych formuł przetargowych, uwzględnianie czynnika innowacyjności w stosowanych kryteriach.

Prawo przedsiębiorców:

- stworzenie możliwości dla wybranego organu do formułowania, w porozumieniu z sektorem NGO, rekomendacji zawierających zestaw klauzul umownych do innowacyjnych projektów z wykorzystaniem technologii IoT przez przemysł.

Prawo danych osobowych:

- uregulowanie gromadzenia i wykorzystania danych maszynowych,

- uregulowanie standardów interoperacyjności urządzeń IoT, np. w drodze rozporządzenia do dyrektywy o swobodnym przepływie danych nieosobowych,

- opracowanie rekomendacji lub innych form *„soft law"* dla przetwarzania danych w chmurze przez Ministerstwo Cyfryzacji we współpracy z Prezesem Urzędu Ochrony Danych Osobowych,

- opracowanie wytycznych (soft law) w zakresie wykorzystywania danych pozyskanych w ramach technologii IoT w sektorze ubezpieczeniowym,

- wprowadzenie do ustawy o działalności ubezpieczeniowej i reasekuracyjnej jednostki redakcyjnej przyznającej ministrowi właściwemu do spraw informatyzacji w porozumieniu z ministrem właściwym do spraw instytucji finansowych kompetencji do wydawania rozporządzenia regulującego kwestie dot. wykorzystywania danych nieosobowych przez sektor ubezpieczeniowy,

- opracowanie przepisów, które będą regulować zagadnienia dotyczące klasyfikowania poszczególnych strumieni danych IoT, sposobu ich ochrony oraz zasad przesyłania i przetwarzania, alternatywą może być wydanie wytycznych w powyższym zakresie przez Ministerstwo Cyfryzacji,

- wyłączenie danych IoT z tajemnic sektorowych oraz wypracowanie nowego sposobu ich traktowania w kontekście przepisów RODO,

- uregulowanie kwestii ubezpieczeń komunikacyjnych opartych o zachowanie kierowców (indywidualne stawki oparte o ocenę stylu jazdy) w ustawie o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych lub ustawy o działalności ubezpieczeniowej i reasekuracyjnej,

- przyjęcie pełnej regulacji, która przeciwdziałałaby dyskryminującemu wykorzystaniu danych, w tym danych medycznych pozyskiwanych przy pomocy systemów IoT,

- wprowadzenie regulacji umożliwiających świadczenie usług telemedycznych za pośrednictwem IoT z wykorzystaniem Big Data i bez ingerencji lekarza, w szczególności gdy jest ona zbędna (np. programy screeningu osób zdrowych, zbieranie danych ze względów epidemiologii) oraz finansowanie tych usług ze środków publicznych,

- wprowadzenie przepisów umożliwiających wykorzystanie danych anonimowych zebranych przez podmioty prywatne od podmiotów publicznej służby zdrowia.

Prawo podatkowe:

- w sprawie kas fiskalnych online zmiana terminologii na gruncie przepisów dotyczących podatku VAT z „urządzenie trwale zawarte w kasie" na „urządzenie trwale zawarte w kasie lub aplikację-usługę dostępną w sieci Internet" oraz dodanie definicji modułu kryptograficznego, pamięci chronionej, opcjonalnie: pamięci fiskalnej w przepisach wykonawczych do ustawy,

- wyniesienie pamięci fiskalnej z urządzenia do warstwy aplikacyjnej w celu redukcji kosztu urządzeń i przyśpieszenia wdrożenia fiskalizacji online oraz nowych metod płatniczych, przy jednoczesnym zmniejszeniu nakładów inwestycyjnych Rządu RP (z 320 mln zł) i przedsiębiorców (z 3 mld zł) w ciągu kolejnych 10 lat,

- wyniesienie pamięci fiskalnej z urządzenia do warstwy aplikacyjnej (np. w chmurze z opcjonalnym zabezpieczeniem kryptograficznym opartym o blockchain) celem przyspieszenia i obniżenia kosztu fiskalizacji online oraz wsparcia adopcji nowych metod płatniczych i e-paragonu.

Bezpieczeństwo:

- rozszerzenie kręgu podmiotów podlegających ustawie o krajowym systemie cyberbezpieczeństwa o wybranych przedstawicieli przemysłu, którzy z racji przetwarzanych danych i skali tego przetwarzania powinni spełniać wyższe wymagania w zakresie cyberbezpieczeństwa,

- analiza i rekomendacje technologiczne w dziedzinie budowania strategii wdrażania aplikacji i tworzenia platform danych,

- wprowadzenie dodatkowych regulacji w zakresie, w jakim Rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej nie odpowiada na wyzwania związane z wykorzystaniem danych anonimowych w IoT,

- opracowanie standardów bezpieczeństwa dla IoT w ustawie o krajowym systemie cyberbezpieczeństwa,

- wydanie „Rekomendacji Ministra Cyfryzacji dotyczących warunków przetwarzania w chmurze publicznej danych podmiotów publicznych" z uwzględnieniem problematyki i specyfiki IoT lub opracowanie innego dokumentu dotyczącego tej tematyki,

- uregulowanie kwestii wykorzystywania danych nieosobowych przez sektor ubezpieczeniowy,

- aktywne włączenie się organów w prace nad regulacją unijną dotyczącą reformy cyberbezpieczeństwa, w szczególności podjęcie prac nad spójnym z regulacją unijną akcie prawnym określającym odpowiedzialność producentów i usługowców medical IoT https://www.consilium.europa.eu/pl/policies/cyber-security/.

Prawo cywilne/zobowiązania:

- rozszerzenie katalogu form zawarcia umowy, w szczególności o formę, w której przedsiębiorca mógłby upoważnić system do automatycznego składania zamówień z wykorzystaniem komunikacji M2M i bez konieczności angażowania w proces osób fizycznych umocowanych do zawierania umów w imieniu przedsiębiorcy.

Prawo administracyjne:

- zmiany w ustawach samorządowych i w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne na rzecz lepszej koordynacji działań jednostek administracji w obszarze technologii IoT oraz popularyzacji wizji Smart City,

- opracowanie strategii rządowej dla rozwoju IoT w Polsce,

- wprowadzenie zmian do ustaw samorządowych w zakresie tworzenia i nadzoru nad spółkami celowymi, tak aby maksymalnie ułatwić dzielenie się infrastrukturą IoT między jednostkami,

- stworzenie i realizacja projektów wykorzystujących IoT w ramach administracji rządowej i samorządowej np. uchwalenie przez Radę Ministrów strategii działania w tym zakresie, która przewidywałaby osiągnięcie konkretnych celów w ramach wdrażania rozwiązań finansowych opartych na IoT,

- opracowanie przez administrację rządową dokumentów z zakresu „*soft law*" (np. wytycznych, standardów lub opinii z zakresu IoT); przygotowanie wzorów dokumentacji w zakresie konkretnych projektów.

Prawo w zakresie transportu i planowania przestrzennego:

- stworzenie ram prawnych do makroskopowego zarządzania transportem, szczególnie w obszarach metropolitalnych i aglomeracjach miast, celem eliminacji narastających problemów zarządzania mikroskopowego, przeprowadzenie pilotażowych zintegrowanych studiów multimodalnych w zaproponowanych (zgodnie z listą przygotowaną przez podgrupę TLPA) obszarach funkcjonalnych miast (aglomeracjach),"

- usunięcie podwójnego obowiązkowego ubezpieczenia odpowiedzialności cywilnej oraz oparcie ubezpieczenia odpowiedzialności cywilnej w związku z ruchem pojazdów autonomicznych wyłącznie na obowiązkowym ubezpieczeniu posiadaczy pojazdów mechanicznych (PPM),

- usunięcie możliwości zgłoszenia sprzeciwu wobec testowania drogowych pojazdów autonomicznych przez właściciela nieruchomości sąsiadującej z drogą, na której pojazdy autonomiczne mają być testowane i zastąpienie regulacją, w której decyzję o zezwoleniu na testowanie pojazdów autonomicznych na drogach publicznych podejmował będzie zarządca drogi, odpowiednio szczebla wojewódzkiego (drogi samorządowe), miejskiego (miasta na prawach powiatu), krajowego (GDDKiA) po zasięgnięciu opinii komendanta wojewódzkiego Policji lub Wojewódzkiego Inspektora Transportu Drogowego; zasadna jest analiza możliwości analogicznego stosowania przepisów o ruchu (drogowym) pojazdów ponadnormatywnych,

- wprowadzenie możliwości testowania pojazdów autonomicznych bez fizycznej obecności kierującego w aucie, np. kontrolującego jego jazdę zdalnie,

- zmiana ustawy Prawo o ruchu drogowym, umożliwiająca stosowanie narzędzi zautomatyzowanego nadzoru nad ruchem (w tym detekcji wykroczeń) przez zarządcę infrastruktury (miasto) w odniesieniu do obszaru objętego ustanowioną strefą czystego transportu,

- umożliwienie tworzenia stref czystego transportu we wszystkich miastach, nie tylko tych powyżej 100 tys. mieszkańców, w szczególności o dużych walorach turystycznych

i uzdrowiskowych oraz zniesienie ograniczeń czasowych co do poboru opłat, opcjonalnie: tworzenie stref czystego transportu w ramach zintegrowanych studiów multimodalnych w aglomeracjach.

Grupa Robocza zgłasza gotowość dalszej pracy nad potrzebnymi zmianami prawnymi, w tym opracowania założeń do zmian ustaw.

Projekty badawczo-rozwojowe

Poniższa lista zawiera propozycje projektów, zgłoszonych przez członków i sympatyków Grupy. Powinny one być traktowane jako wstęp do dalszej dyskusji. Wybrane projekty będą przedmiotem kontynuacji prac Grupy od czerwca 2019 r. Zainteresowanych działaniami w tym obszarze zapraszamy do współpracy.

Na poziomie wspólnym dla wszystkich branż grupa wskazała, że konieczne jest:

- opracowanie zaleceń dla uczelni otwierających kierunki studiów związane z technologią IoT, w zakresie kształcenia ekspertów o adekwatnych do potrzeb rynku umiejętnościach (moja propozycja – do akceptacji/modyfikacji),
- stworzenie przy Ministerstwie Cyfryzacji inkubatora projektów IoT,
- stworzenie Krajowego/Zintegrowanego Systemu Wspierania Innowacji, który prowadziłby innowatorów „od pomysłu do przemysłu”,
- stworzenie mechanizmu finansowania innowacji polegającego na dofinansowaniu wdrożeń pilotażowych i projektów PoC dla użytkowników końcowych, obejmującego innowacyjne produkty zarówno startupów jak i firm dojrzałych,
- zapewnienie odpowiedniej infrastruktury do przesyłania urządzeń IoT oraz do przechowywania i przetwarzania danych.

Godne rozważenia są też pomysły projektów branżowych.

Bezpieczeństwo i Certyfikacja

- zbudowanie jednego, wspólnego słownika pojęć IoT, który będzie używany w całej legislacji, a także w dokumentach normatywnych, najlepszych praktykach i materiałach edukacyjnych,
- wypracowanie norm w zakresie bezpieczeństwa, interoperacyjności i standaryzacji oraz metod ich certyfikacji.

Transport, Logistyka i Pojazdy Autonomiczne

Planowanie transportu multimodalnego / zintegrowanego:

- zintegrowane terytorialne planowanie sieci transportowej,
- planowanie optymalnych multimodalnych tras podróży i dostaw (uwzględniając pojazdy autonomiczne), z wykorzystaniem danych urządzeń IoT,
- zastosowanie IoT do redukcji zanieczyszczeń z transportu, np. planowanie i obsługa stref czystego transportu,
- powiązanie z innymi elementami Smart City w aglomeracjach,
- analiza symulacyjna ruchu pojazdów autonomicznych i systemów transportu autonomicznego z uwzględnieniem suboptymalizacji wielokryterialnej oraz wrażliwości strukturalnej i parametrycznej, ze szczególnym uwzględnieniem specyfiki polskich miast.

Finanse i Ubezpieczenia

- dialog techniczny i pilotaż nowej architektury wymiany informacji z Internetem i kryptograficznie zabezpieczonego zapisu danych paragonowych poza chronioną pamięcią fizyczną kasy fiskalnej,

- wypracowanie nowych metod płatności za transport publiczny poprzez instalację i standaryzację czujników typu bluetooth beacon w pojazdach komunikacji miejskiej oraz na przystankach,

- upowszechnienie w sektorze ubezpieczeń rozwiązań, opartych na wykorzystaniu telematyki czasu rzeczywistego dla danych z pojazdów, w tym o lokalizacji, użyciu bądź postoju pojazdu i bezpieczeństwie stylu jazdy kierowcy.

Inteligentne Miasta i Budynki

Stworzenie ogólnopolskich ram interoperacyjności Smart City.

Ochrona Zdrowia

Narodowy system do zapewnienia cybernetycznej, chmurowej opieki nad dużą populacją chorych (do zbudowania na bazie wersji demonstracyjnej powstającej w ramach Demonstratora 1.1.2 NCBiR).

Rolnictwo i Ochrona Środowiska

- budowa sieci stacji agrometeorologicznych w kraju – rozbudowa istniejącej w części kraju sieci ODR, umożliwiająca gromadzenie danych o ryzykach, agregowanych w rolniczej chmurze danych i udostępnianych przez API,

- monitorowanie stanu pszczół w Polsce – stworzenie konkurencyjnego krajowego rozwiązania do monitorowania umożliwiającego pszczelarzom zapewnienie zdrowia pszczołom poprzez kontrolowanie warunków bytowania owadów w ulach, takich jak temperatura, wilgotność czy wykrywanie chorób oraz opracowanie systemu zarządzania pasieką i wspomagania decyzji, a także opracowanie mapy „upszczelenia" obszarów kraju,

- monitoring jakości powietrza w oparciu o niskokosztowe czujniki jakości powietrza kalibrowane względem stacji referencyjnych – rozbudowa sieci uzupełniającej Państwowy Monitoring Środowiska pozwoli na pozyskiwanie wielu informacji niemożliwych dotąd do osiągnięcia na bazie Państwowego Monitoringu Środowiska.

Przemysł

- projekt badawczy (TRL I-VI) oraz w drugiej kolejności projekt rozwojowy (TRL VII-IX) – budowa otwartej platformy do wymiany danych dostępnych dla uczestników rynku i firm technologicznych,

- projekty budowy testowej drogi Polska – Litwa wykorzystującej technologie IoT do testowania pojazdów autonomicznych; Implementacja modelu innowacyjnych usług w tym usług ubezpieczeniowych w nowej rzeczywistości funkcjonowania samochodów autonomicznych,

- dedykowany program Scale Up dla rozwoju IoT w Polsce.

Grupa Robocza ds. IoT – członkowie, obserwatorzy i sympatycy

Poniższa lista zawiera osoby, które aktywnie uczestniczyły w posiedzeniach Grupy ds. IoT i/lub brały udział w pracach redakcyjnych zdalnie (zgłaszały uwagi bezpośrednio do Zespołu Redakcyjnego MC lub do liderów podgrup).

Bezpieczeństwo i Certyfikacja

Lider – Czarnowski Aleksander, AVET Information and Network Security
Jakubiak Adam, Polkomtel
Karpiński Andrzej, Orange Polska
Kowalczuk Konrad, MGK.net.pl
Krauze Michał, T-Mobile Polska S.A.
Kubiak Wojciech, GASPOL S.A.
Kuczorski Arkadiusz, Oracle
Łazarz Łukasz, CAN-PACK S.A.
Oko Jacek, Politechnika Wrocławska
Piotrowski Andrzej, UTC Fire & Security Polska
Radawiec Rafał, Politechnika Wrocławska
Steczowicz Bartłomiej, Teraz Energia
Więckowska Mariola, LexDigital
Zarembiński Jakub, Sygnet

Finanse i ubezpieczenia

Lider – Wolski Marcin, startup Billon Group
Brozowski Piotr Jan, Krajowa Izba Doradców Podatkowych
Kluwak Tomasz, Krajowa Izba Doradców Podatkowych
Krzywania Przemysław, BKF Myjnie Bezdotykowe
Kuna Mariusz, Polska Izba Ubezpieczeń
Kwieciński Michał, Platforma Detalistów
Leciejewski Maciej, Regent Insurance Brokers (Polska)
Panufnik Tomasz, Dell EMC|Public
Zacharjasz Igor, Inkubator Innowacji Visa

Inteligente miasta i budynki

Lider – Wiśniewski Remigiusz, Detecon International GmbH
Bakalarz Rafał, Netia
Bałos Michał, EmiTel S.A.
Bergmann Krystian, Fibar Group S.A.
Chomiczewski Witold, Izba Gospodarki Elektronicznej
Choroś Patryk, SAS Institute
Czuszek Krzysztof, Stowarzyszenie e-Południe – EPIX
Gamza Zbigniew, Miejskie Centrum Przetwarzania Danych – Wodzisław Śląski
Jarosiewicz Mateusz, Smart Cities Polska
Kamysz-Turbak Marta, Urząd Miasta Tarnobrzeg
Klimas Damian, Uniwersytet Wrocławski
Kołoszczyk-Jakubowski Tomasz
Kraska Marcin, Instytut Logistyki i Magazynowania
Maroszek Franciszek, Nokia Solutions and Networks / Stowarzyszenie Hackerspace Wrocław
Leśniak Klaudia, Indoorway
Orchowski Kacper, Deloitte Consulting
Pietrzak Roman, ITI EMAG
Polski Mirosław, Hewlett-Packard Enterprise Polska
Serafin Marcin, Kancelaria Maruta Wachta
Stefański Mateusz, Microsoft
Urbaniak Maciej, Ministerstwo Inwestycji i Rozwoju
Wierzejski Arnold, Nokia

Ochrona zdrowia

Lider – Bień Krystian, Polpharma sp. z o.o., Akademia Leona Koźmińskiego
Jackowski Michał, DSK Kancelaria i LexDigital
Kołc Bogusław, PZU Zdrowie S.A.
Komar Michał, kancelaria prawna D. Dobkowski
Kurasiński Michał, Polpharma sp. z o.o.
Niewiadomski Bartosz, Grupa Aviva
Talarek Piotr, TBT i Wspólnicy
Wiktor Dawid, kryptoinwestor
Zwoliński Piotr, Uczelnia Łazarskiego

Ogólna

Liderzy: Zamłyński Marek, IDC (do grudnia 2018); Mieczkowski Piotr, Fundacja Digital Poland
Smulski Jarosław, IDC
Besiekierska Agnieszka, Kancelaria Noerr Biedrecki
Dyśko Mateusz, Peter Nielsen & Partners Law Office Sp.k.
Federowicz Rafał, federowicz.eu
Gałęzowska Karolina, PwC Legal
Grabia Michał, Instytut Logistyki i Magazynowania
Hryszko Arnika, Stowarzyszenie Jakości Systemów Informatycznych
Hryszko Jarosław, Stowarzyszenie Jakości Systemów Informatycznych
Gałagus Michał, Polska Izba Informatyki i Telekomunikacji
Kocięcki Maciej, Orange Polska
Konarski Xawery, Kancelaria Traple Konarski Podrecki i Wspólnicy
Mednis Arwid, PwC Legal / Uniwersytet Warszawski
Matysiak Michał, Kancelaria Traple Konarski Podrecki i Wspólnicy
Mińkowski Marcin, Oracle
Sikorski Marcin, Stowarzyszenie Jakości Systemów Informatycznych
Stokalski Borys, Polska Izba Informatyki i Telekomunikacji

Inteligentne opomiarowanie

Lider – Wadas Krzysztof, Grupa Cyfrowy Polsat
Chorążyczewski Artur, Revive Machines
Falandysz Jaromir, ENERGA, Towarzystwo Obrotu Energią
Gabryś Marek, AIUT
Galant Marek, Revive Machines
Galas Paweł, Orange ENERGA, Towarzystwo Obrotu Energią
Golik Piotr, T-Matic Systems S.A
Gręblicki Jerzy, AIUT
Grochla Krzysztof, Instytut Informatyki Teoretycznej i Stosowanej PAN
Jankowski Andrzej, Aquard
Kotewicz Radosław, Comarch S.A.
Kowalski Rafał, Diehl Metering
Pietrzyk Slawomir, IS-Wireless
Ratyński Mikołaj, T-Mobile Polska
Smoliński Rafał, Yoberi
Ślęczek Wojciech, Polkomtel
Wądołowski Piotr, T-Matic Systems S.A.
Zawadzka Anna, kancelaria prawna Lewandowska

Przemysł
Lider – Nawrocki Kamil, Bconnect
Boniecki Szymon, Monterail
Gliszczyńska Beata, PZU Lab S.A.
Gołębiewski Dariusz, PZU Lab S.A.
Iwaniuk Maciej, Ernst & Young
Kuczyński Marek, PZU Lab S.A.
Łobaziewicz Monika, Uniwersytet Warszawski
Nachyła Dariusz, Every European Digital
Serafin Tomasz, AIUT
Ślęk Bogdan, Signify Poland
Widórek Jarosław, Comarch S.A.
Zalewski Tomasz, kancelaria Bird & Bird

Rolnictwo i ochrona środowiska
Lider – Płóciennik Marcin, IChB PAN Poznańskie Centrum Superkomputerowo Sieciowe
Białousz Jerzy, Inventia
Mańkowski Rafał, Polska Izba Ubezpieczeń
Misiek Michał, Airly
Kolasiński Michał, Agrospot
Kowalski Piotr, Orange Polska
Pietroń Jakub, JMLabs
Poniewierski Aleksander, Ernst & Young
Prądzyński Michał, Agrotechnology
Rajtar Tomasz, IChB PAN Poznańskie Centrum Superkomputerowo Sieciowe (PCSS)

Telekomunikacja
Lider – Michalski Mateusz, mTechnology / Stowarzyszenie Hackerspace Wrocław
Barcikowski Michał, T-Mobile Polska
Dylik Tomasz, Exatel
Dziomdziora Wojciech, Kancelaria prawna Domański Zakrzewski Palinka
Gęsiak Przemysław, Polkomtel
Gorzkowska Katarzyna, AP Law
Górski Janusz, T-Mobile Polska S.A.
Grabowski Sebastian, Orange Poland
Kogut-Czarkowska Magdalena, Związek Pracodawców Branży Internetowej IAB Polska
Kozłowski Krzysztof, Orange labs
Modelski Józef, Politechnika Warszawska
Mroczkowski Jarosław, EmiTel S.A.
Piechocki Artur, Sąd Polubowny ds. Domen Internetowych przy PIIT
Staszak Maciej, EmiTel
Sugak Marcin, Ericsson

Transport, logistyka i pojazdy autonomiczne
Liderzy – Gora Paweł, Uniwersytet Warszawski
Hajduk Damian, doradztwo strategiczne i zarządzanie w transporcie i logistyce
Chłopik Monika, Polska Izba Ubezpieczeń
Choromański Włodzimierz, Politechnika Warszawska
Darowska Małgorzata, Ministerstwo Infrastruktury
Domański Marcin, Fundacja Napraw Sobie Miasto
Dzięcielski Michał, Uniwersytet im. Adama Mickiewicza w Poznaniu
Gawliczek Łukasz, Ave Cargo
Grabarek Iwona, Politechnika Warszawska
Grabowski Waldemar, Uniwersytet Zielonogórski / Stowarzyszenie Nauczycieli Fizyki SNaFi
Horzela Agata, GS1 Polska
Jacyna Marianna, Politechnika Warszawska
Klusek Michał, Główny Urząd Geodezji i Kartografii
Konert Anna, Uczelnia Łazarskiego
Kosiło Tomasz, Politechnika Warszawska
Kostrzewa Konrad, Veturai Automotive Sp. z o. o.
Kruszewski Mikołaj, Instytut Transportu Samochodowego
Krystyniecka-Konopczak Magdalena, Polskie Linie Lotnicze LOT S.A.
Krzykowska Karolina, Politechnika Warszawska
Malinowski Zbigniew, Geo-System
Matysiak Arkadiusz, Instytut Transportu Samochodowego
Mazur Bartosz, Fundacja Napraw Sobie Miasto
Moskwa Radosław, CM Logistic
Orzechowska Renata, Polska Izba Ubezpieczeń
Przecherski Piotr, Olczak – Klimek, Van der Kroft, Węgiełek Kancelaria Radców Prawnych
Siergiejczyk Mirosław, Politechnika Warszawska
Stańczyk-Miścicka Paulina, Urząd Lotnictwa Cywilnego
Szafrański Zbigniew, Doradztwo Kolejowe
Szarata Andrzej, Politechnika Krakowska
Szustek Jarosław, Tramwaje Warszawskie
Wilczewski Grzegorz, DAWIS IT Sp. z o.o.
Wolniewicz-Warska Ewa, Kapsch Telematic Services

Ponadto gośćmi specjalnymi Grupy IoT na pojedynczych posiedzeniach byli:

24.08.2018 – Inauguracja prac Grupy – Minister Karol Okoński, Sekretarz Stanu, Ministerstwo Cyfryzacji i Minister Marcin Ociepa, Podsekretarz Stanu, Ministerstwo Przedsiębiorczości i Technologii.
16.10.2018 – Tomasz Jamróz, Radca, Departament Współpracy Ekonomicznej, Ministerstwo Spraw Zagranicznych (Polish Technology Hub – szanse polskich technologii IoT na forum międzynarodowym).
06.11.2018 – Waldemar Izdebski, Główny Geodeta Kraju (Możliwości przestrzennej wizualizacji danych i potencjał systemów GUGIK dla polskiego biznesu w aspekcie IoT).
04.12.2018 – reprezentanci siostrzanych grup roboczych w MC: Grupy ds. Otwartości Danych – (Nowa dyrektywa o ponownym wykorzystywaniu ISP i propozycja katalogu danych wysokiej wartości) oraz Grupy ds. AI – Michał Pukalak koordynowanej przez Departament Polityki Międzynarodowej.
22.01.2019 – Luiza Modzelewska, Zastępca Dyrektora Departamentu Doskonalenia Regulacji Gospodarczych, Ministerstwo Przedsiębiorczości i Technologii (przedstawiła koncepcję Prostej Spółki Akcyjnej (PSA)) i dr inż. Elżbieta Andrukiewicz, Instytut Łączności (Certyfikacja urządzeń IoT – normy referencyjne oraz pierwsze inicjatywy).
05.03.2019 – Małgorzata Darowska, Pełnomocnik Ministra Infrastruktury ds. Bezzałogowych Statków Powietrznych i programu Centralnoeuropejski Demonstrator Dronów, Ministerstwo Infrastruktury (Biała Księga BSP) oraz Jarosław Rupiewicz, Departament Bezzałogowych Statków Powietrznych, Urząd Lotnictwa Cywilnego (Przepisy dla lotów Bezzałogowych).

POWSTAJE

POLSKA INTERAKTYWNA MAPA INNOWACJI

Sprawdź co robią sąsiedzi.

Dodaj swój projekt!

Wejdź na stronę:

www.gov.pl/web/uslugi/mapa-innowacji