DOI: 10.15199/13.2017.6.1

Internet Przedmiotów – od nauki do przemysłu

(Internet of Things – from research to industry)

prof. dr hab. inż. RYSZARD S. ROMANIUK

Politechnika Warszawska, Instytut Systemów Elektronicznych, Wydział Elektroniki i Technik Informacyjnych
Ryszard.Romaniuk@cern.ch

Streszczenie

Internet Przedmiotów, Internet Rzeczy, Internet of Things staje się odrębną interdyscyplinarną dziedziną nauki i techniki integrującą takie obszary jak informatykę, telekomunikację, elektronikę i fotonikę, nauki informacyjne, psychologię i socjologię, nauki ekonomiczne, nauki o biznesie i gospodarowaniu. Korzysta z rozwoju tych nauk wprowadzając nową jakość. Część Internetu Przedmiotów dotycząca bezpośrednio człowieka nazywamy Internetem Dotykowym, Internetem Socjalnym, lub Internetem Usługowym. Część Internetu Przedmiotów integrowana z funkcjonalnymi warstwami cywilizacyjnymi nazywamy Internetem Infrastrukturalnym lub Internetem Inteligentnej Infrastruktury. Oba te Internety zostały nazwane przez Cisco, a termin przyjął się szerzej, Internetem Wszystkiego, Internet of Everything IoE. Autor przedstawia ogólniejsze monograficzno-eseistyczne, nieco subiektywne, wprowadzenie do Internetu Rzeczy, także bazujące częściowo na własnych doświadczeniach budowy takiego Internetu dla wielkich eksperymentów badawczych w CERN, GSI, FAIR, w ramach akceleratorowych projektów Europejskich CARE, TIARA, EuCARD, ARIES. Takie i inne doświadczenia badawcze są obecnie nadspodziewanie intensywnie transferowane do życia codziennego i przemysłu. Taki przemysł określamy nawet odrębnym terminem jako Przemysł w wersji 4.0.

Słowa kluczowe: Inżynieria sieci web, Inżynieria Internetu, Internet, Internet Przedmiotów, Internet Rzeczy, IoT, Przemysł 4.0, Technologie Mgły i Chmury, Wielkie Zbiory Danych, sieć WWW, funkcjonalne sieci inteligentne i kognitywne, inteligencja obliczeniowa, sztuczna inteligencja

Abstarct

Internet of Things – IoT – turns to a strongly defined and separate, interdisciplinary branch of science and technology. It integrates such areas as: informatics, telecommunications, electronics and photonics, information sciences, psychology and sociology, economic sciences, and business sciences. IoT benefits from the development of these sciences introducing its strongly visible own quality. The part of of the IoT which concerns directly human beings is called Tactile Internet, Internet of Tactile Things, Internet of Social Things, Internet of Services, etc. The part of IoT which is integrated with the solid functional layers of our civilization is called Infrastructural Internet, Internet of Infrastructural Things, or just Intelligent Infrastructure. These both Internets were called by Cisco, ant this term was accepted widely, the Internet of Everything or IoE. The author presents here a more general monographic essay, slightly subjective consideration, which is an introduction to the Internet of Things. These considerations are based, at least partly, on own experiences of development and introduction of such Internets for large research experiments in CERN, GSI, FAIR, and in the framework of the European accelerator infrastructural projects like CARE, TIARA, EuCARD, ARIES. Such ones and other research experiences are now surprisingly efficiently transferred to the everyday life and the industry. Such an industry is even given a special version and called Industry 4.0.

Keywords: Web engineering, Internet engineering, Internet, Internet of Things, IoT, Industry 4.0, Cloud and Fog technologies, Big Data, WWW network, intelligent and cognitive functional networks, computational intelligence, artificial intelligence

Internet Przedmiotów jest jednocześnie zjawiskiem społecznym, specjalnością naukową i techniczną, tworzoną obecnie specjalnością przemysłową, staje się częścią przebudowywanej i budowanej od nowa infrastruktury cywilizacyjnej, a także kultury. Może łatwiej powiedzieć, być może z pewną przesadą, czym Internet Przedmiotów nie jest. Równocześnie z przedstawieniem wielostronności skomplikowanego podłoża technicznego tego zjawiska pokazujemy subiektywnie, w różnych aspektach, być może nieco futurystycznie i filozoficznie, jego otoczenie. Bazujący na wielu obszarach wiedzy i budowany od niespełna dwudziestu lat Internet Przedmiotów może być przedstawiany w bardzo różny sposób pod względem ekonomicznym, architektonicznym i technicznym, także humanistycznym. Niektórzy, pół żartem, pół serio mówią, że transformuje nam cywilizację, do czego odniesiono się skrótowo i niesystematycznie we wstępie o 'Internetyzacji cywilizacji'. Naukowo techniczne podłoże Internetu Przedmiotów jest stosunkowo bogate, z czego skorzystano przedstawiając to zjawisko w części 'Definicje' z punktu widzenia informatyki, telekomunikacji, elektroniki, czy inżynierii komputerowej, ale także ontologii. Dowodem na złożoność strukturalną Internetu Przedmiotów jest bardzo bogata literatura naukowa i społecznościowa na jego temat, obejmująca gospodarkę, zdrowie, środowisko, rozrywkę i kulturę, socjologię, a także nauki humanistyczne. Internet Przedmiotów rozwija się dynamicznie i w dużej mierze spontanicznie, wykorzystując zapotrzebowanie rynku i duże inwestycje indywidualne oraz zorganizowane, internetowe, grupowe. Obszar ten jest zagospodarowywany od pewnego czasu w sposób bardziej uporządkowany przez instytucje standaryzacyjne i techniczne, finansowe i gospodarcze, naukowe i przemysłowe, oraz społecznościowe. Ktoś musi tutaj zrobić porządek, co przedstawiamy w części pracy 'Organizacje'. Internet Przedmiotów, mimo powszechnego rozumienia go jako warstwy martwej, maszynowej, jest obszarem działania i intensywnego, wielokierunkowego oddziaływania z człowiekiem. Część 'Człowiek a Internet Przedmiotów' wydaje się najważniejsza, pokazując wybrane drogi nowego wpływu inteligentnej techniki na człowieka, i odwrotnie, a przez to być może tworzenia rodzaju cyfrowego ludzkiego pokolenia przyszłości. Więcej informacji technicznych, co jest być może uzasadnione tematyką pracy, czyli nowoczesny przemysł i jego zawiłe ścieżki przekształcania z warstwy nauki i innowacji, zebrano w części 'Transformacja', zapewne nieco mniej czytelnej dla osób nietechnicznych. W kopernikańsko-galileańskim zakończeniu pracy ponownie straszymy czytelnika zagrożeniami ze strony Internetu Przedmiotów, który kiedyś zamieni się w, miejmy nadzieję, przyjazne dla człowieka Inteligentne Środowisko. W całej pracy rozsiane są różne, nieuporządkowane przykłady mniejszych i większych, mniej i bardziej ważnych czy przydatnych aplikacji Internetu Przedmiotów, niektóre z nich czasami humorystyczne. Rozsiane są także terminy i popularnie używane skróty specyficzne dla Internetu Przedmiotów, zgodnie z zasadą że każda dziedzina wypracowuje swój specyficzny język bez którego nie istnieje. Niestety pełne wyjaśnienie wszystkich terminów nie było tutaj możliwe, gdyż taka pełniejsza praca o Internecie Przedmiotów musiałaby mieć kilkaset stron. Usunięcie specyficznego języka Internetu Przedmiotów znacznie spłycałoby pracę. Używane terminy i skróty języka IoT są obecnie już tak popularne, że zupełnie niepotrzebne jest podawanie ich odnośników internetowych. Proste zapytanie natychmiast daje pełne wyjaśnienie. Zamierzeniem autora, i wydaje się że także wydawnictwa, było przedstawienie gęstego ujęcia monograficznego o IoT jednak szerokiego, dostatecznie treściwego, pełnego danych, aplikacyjnego i technicznego, ale z odniesieniem do otoczenia pozatechnicznego, profesjonalnego ale jak najbardziej zrozumiałego. Znaczna refleksyjność i ilość treści subiektywnych w tekście, a także pewna asocjacyjność i niesystematyczność wywodu wydaje się kwalifikować go jako rodzaj skromnego, perswazyjnego eseju techniczno-humanistycznego. Perswazyjnego, bo niezdarnie przekonującego czytelnika do poglądu, że Internet Przedmiotów to sprawa nietrywialna, więc zasługuje zdecydowanie na napisanie przez humanistów jak najprędzej prawdziwego, poważnego, wyczerpującego eseju li-

teracko-naukowego w języku polskim, bazującego na naszych krajowych doświadczeniach, i o dobrze przemyślanym ładunku humanistycznym. Takiego oryginalnego dzieła po Polsku jeszcze nikt nie odważył się napisać. Bez zrozumienia potencjalnie fundamentalnej wagi rozwijającego się lawinowo Internetu Przedmiotów dla humanizmu i cywilizacji nie można go dokładnie opisać. Opisujemy wówczas jedynie skomplikowany przedmiot, podczas gdy być może już nawet my, nasze pokolenie, a na pewno następne będzie świadkiem jego upodmiotowienia i zmiany statusu w obserwatora. Transformacja Internetu Przedniotów ex scientia et industria posiada wiele różnych ścieżek, dróg i autostrad, prostszych i bardziej skomplikowanych. Część tego systemu tworzy skomplikowany labirynt. Nie wszystkie drogi tego labiryntu prowadzą we właściwym kierunku. Niektóre, ginąc za horyzontem poznania, prowadzą nie wiadomo gdzie. Niektóre, krótsze mają na końcu wyraźniej zarysowany cel. Wydawałoby się, że to takie proste. Mamy znakomite osiągnięcia na polu nauki w wielu obszarach zainteresowania Internetu Przedmiotów, nic tylko szybko je uprzemysłowić, powszechnie zastosować i korzystać! I tak się dzieje w wielu obszarach, do których prowadzą zatłoczone drogi. Czasami przeszkody w akceptacji IoT są natury psychicznej, czy pokoleniowej, bo jak tu uznać od razu blockchain, zdecentralizowany, bezserwerowy i najpopularniejszy na świecie portfel waluty bitcoin za swój (blockchain.info). Zaczynamy także zauważać inne ciekawe atrybuty tego zjawiska, nie dające opisać się w sposób uproszczony. Antropomorfizując to zjawisko, choćby częściowo i ostrożnie dodając już w pełni usprawiedliwioną cechę kognitywną, co zdarzy się jeszcze kilkukrotnie w tym stanowczo zbyt długim tekście, staramy się opisać je a capite ad calcem. Internet Rzeczy jest wdzięcznym tematem do pisania o nim. Nie jest nauką hermetyczną w związku z czym nie wymaga stosowanego, ścisłego wprowadzenia naukowo-formalnego, chyba że jest to prologomena do wszelkich nauk niehermetycznych. Do tego rodzaju rozważań wstępnych aspiruje ten tekst. Podłożem Internetu Rzeczy jest oczywiście piękna technika, ale nie ona w ostatecznym rozrachunku zadecyduje o zrozumieniu i akceptacji społecznej. Prawie każdy obszar Internetu Rzeczy posiada bowiem, lub będzie posiadać, zakotwiczenie społeczne i humanistyczne.

IoT-yzacja cywilizacji, verum aut falsum?

Co dała nam era cyfrowa? Milionowe przyspieszenie tworzenia, zbierania, transmisji, i przetwarzania informacji. Co da nam era kwantowa, jeśli nadejdzie. Dalsze milionowe, może miliardowe przyspieszenie w porównaniu do ery cyfrowej. Internet Przedmiotów, określany skrótem IoT, jest spóźnionym dzieckiem ery cyfrowej. IoT jest niespełnioną jeszcze obietnicą ery kwantowej. Dlaczego spóźnionym, przecież mógł być rozwijany wcześniej? Dlatego być może, że szok po zrozumieniu możliwości cyfrowego przetwarzania danych, wymagał najpierw nadrobienia zaległości technicznych, pokonania barier nietechnicznych, rozglądnięcia się po potencjalnych zastosowaniach, ochłonięcia psychicznego. Dlaczego obietnicą? Inteligencja obliczeniowa IoT bazująca na przetwarzaniu wielkich ilości informacji miliard razy sprawniej od obecnej przekroczy znacznie inteligencję człowieka. A jeśli przekroczy, to zmieni się cała cywilizacja ludzka. A to że przekroczy, dzisiejsza nauka nie ma wątpliwości. Dzisiaj brzmi to, dla osoby spoza nauki, obrazoburczo, prawda? Internet Przedmiotów, Internet Rzeczy, Internet Obiektów, Internet Infrastruktury, Internet Dotykowy, Internet Socjalny, Internet Konsumencki, Internet Przemysłowy, Internet Kooperatywny, wreszcie Big Data Internet i Internet Wszystkiego, ale również komunikacja międzymaszynowa M2M, także Fog Computing, czy Przemysł 4.0, Cloud Computing, środowiska programistyczne do cyfryzacji biznesu jak SMAC – Social, Mobile, Analytics and Cloud computing, środowiska usługowe AWS –Amazon Web Services, Microsoft Azure, IBM Watson, i inne, obecnie w literaturze globalnej określany zadziwiająco jednolicie, jako Internet of Things, jest dziedziną interdyscyplinarną, nie tylko pod względem technicznym. Mówi się, że termin IoT został użyty po raz pierwszy przez Kevina Ashtona, jednego z twórców standardu RFID, w roku 1999. Popularność Internetu Przedmiotów jest tak duża, że ustanowiono międzynarodowy Dzień IoT na 9 kwietnia (iotday.org). W roku 2017 będzie obchodzony konferencyjnie w różnych miejscach świata przez różne organizacje po raz piąty. Powstał termin klucz IoT, otwierający drzwi do nowej wiedzy, a także do biznesu, pieniędzy i transformacji społeczeństwa. W obszarze techniki, czyli swojego podstawowego podłoża materialnego, IoT korzysta obficie z rozwoju takich dziedzin jak elektronika i telekomunikacja, inżynieria materiałowa i mechatronika, czujniki i metrologia, oraz oczywiście inżynieria komputerowa i informatyka. W obszarze granicznym techniki i humanizmu IoT korzysta z nauk i technik informacyjnych, socjologii, oraz mediów, przyczyniając się w nowy sposób do ich rozwoju. Wręcz integruje ten rozwój w nową całość, nową jakość. Efektem tej interdyscyplinarności, a więc prawie nieograniczonego korzystania z postępu wielu dziedzin nauki i techniki, jest gwałtowny rozwój techniczny i pozatechniczny IoT. Tak gwałtowny, że napotyka istotne bariery społeczne i psychologiczne w zastosowaniach praktycznych, szczególnie takich w bezpośrednim otoczeniu człowieka. Te bariery i ich atrybuty są przedmiotem badań. IoT otacza człowieka coraz bliżej, i ten dystans się zmniejsza, więc mamy do czynienia z takimi zjawiskami pozytywnymi i negatywnymi, wszystkie z atrybutem cyfrowy, nie do pominięcia w niedalekiej przyszłości jak: bliskość i dotyk, lęk, nałóg, histeria, ideologia, wyobcowanie, przesądy, zafascynowanie, edukacja, kształcenie, generacja, pokolenie, wizja, predykcja, bezpieczeństwo, zagrożenie, zanurzenie, itp. Oddzielenie IoT od człowieka oznaczałoby że zupełnie nie rozumiemy tego co się dzieje obecnie wokół nas. IoT zarządzający obecnie ruchem drogowym, firmą, mostem, klimatyzacją i lodówką, a w przyszłości całym otoczeniem, wydaje się dość prymitywny i daleki od człowieka, to złudzenie, tak nie jest. IoT jest przyszłym atrybutem osobistym człowieka i jego cywilizacji, ale przede wszystkim człowieka. IoT będzie emanacją i znacznym rozszerzeniem inteligencji i osobowości człowieka. IoT będzie projekcją inteligencji człowieka na przestrzeń wielowymiarową, czterowymiarową fizyczną x-y-z-t, i nie wiadomo ile wymiarową społeczną, psychiczną, kulturalną, religijną. Dzisiaj brzmi to być może nieco obrazoburczo dla niektórych, prawda? Zdarzy się wcześniej niż myślimy. Być może czeka nas zdetronizowanie inteligencji i oddzielenie jej od człowieka. Człowieczeństwa będziemy poszukiwali w innych atrybutach ludzi. Nie w inteligencji, w sercu. Tak jak w Przewrocie Kopernikańskim zdetronizowano Ziemię. E-religia, Internet w służbie religii a może religia w służbie Internetu, o przenoszeniu religijnych granic do cyberprzestrzeni, czy Internet i IoT są zagrożeniem dla Kościoła, gdzie Kościół nie może tam Internet pośle, Internet potrzebny na lekcjach religii, immersyjne uczestnictwo w obrzędach religijnych, o nietrwałości podziału na świat online i offline, o tym że świat staje się hybrydą rzeczywisto-wirtualną, Internetowe ścieżki donikąd, to są prawdziwe, współczesne i twarde tematy badawcze psychologów, socjologów religii i kultury. Zauważamy wiele pułapek na tej skomplikowanej drodze początkowego rozwoju IoT. Mówimy na przykład o niebezpieczeństwach, postępującej pladze gadżetomanii internetowej, o uzależnieniu, o śmieciowisku, o ciemnych zakamarkach, gdzie człowiek chce internetyzować wszystko wokół siebie, o cyberbezpieczeństwie, o wielkich kosztach środowiskowych przyszłego IoT. Ale także mówimy o niepohamowanej pasji twórców IoT. Dokłada się do tego także przemysł pragnący zaspokoić popyt, w wielu przypadkach sam go kreując, czasami uczciwie, czasami nieco mniej uczciwie, w każdym przypadku często coraz bardziej agresywnie.

Sieć globalna Internet powstawała początkowo w środowiskach naukowych i wojskowych. Nadal jest tam intensywnie rozwijana, ale obecnie w zupełnie inny sposób niż w czasach pionierskich, kilkadziesiąt lat temu. Badane są atrybuty szczególnie przydatne w tych obszarach jak np. determinizm transmisji, sub-nanosekundowa precyzja czasowa, współpraca z systemami operacyjnymi czasu rzeczywistego, masowa skalowalność sprzętowa i informatyczna, nowe standardy techniczne, czy szczególnie wysoki poziom niezawodności, odporność na specjalne warunki pracy. Dzisiaj, gwałtownie rozwinięta masywność powszechnych zastosowań Internetu, we wszystkich jego odmianach, zamkniętych i otwartych, dostępnych i niedostępnych, powszechnych i profesjonalnych, komercyjnych i społecznościowych, także sieci web, chmury, intranetu, Ethernetu, internetowych hurtowni danych, Internetu Rzeczy, przemysłowego, medycznego, zmienia bardzo wiele wokół nas. Mówimy że Internet Przedmiotów, cicha inteligencja wręcz rozlewa się wszędzie zmieniając kierunki i przyspieszając przemiany cywilizacyjne. Penetruje infrastrukturę i wiele obszarów działalności społeczeństwa, także sport, edukację i kulturę. Rozwijane w różnych środowiskach naukowych, społecznościowych i przemysłowych, odmienne cechy IoT wydają się ostatecznie spotykać w wielu aplikacjach powszechnych. IoT powstaje wszędzie, rozwijany także w środowiskach poza-profesjonalnych, amatorskich. Zadajemy pytania dotyczące IoT. Gdzie i jak powstaje? Jaka jest jego ogólna struktura? Jak się transferuje pomiędzy nauką i przemysłem? Co nam taki rozwój daje? Jak wspomoże rozwój cywilizacji? A konkretnie: Czy poprawi nasz dobrobyt, służbę zdrowia, przyspieszy poznawanie świata, zmieni edukację, zmieni biznes i przełoży się efektywnie na rozwój gospodarczy? Pytamy jeszcze bardziej szczegółowo: czy

i w jaki sposób rozwijane obecnie technologie w obszarze inżynierii materiałowej, elektroniki, fotoniki, mechatroniki, telekomunikacji, automatyki i robotyki, oraz informatyki, czyli sprzętu i oprogramowania, dadzą się zagospodarować w bardziej dojrzałe i przydatne produkty funkcjonalne IoT? Jesteśmy dopiero na początku, odkryliśmy IoT i jego niektóre składowe jak sztuczną inteligencję zaledwie chwilę temu. Wiele z osiągnięć technologicznych pozostaje jeszcze nie przetłumaczonych na praktyczny język IoT. Przyglądniemy się tym możliwościom, raczej ograniczając się do poziomu naukowo-technicznego i redukując rozważania do tego co jest dzisiaj już dostępne lub jest prawie osiągalne. Podłożem technicznym IoT jest sieć, praktycznie bez ograniczeń różnorodności, przepustowości, sposobów dostępu i ruchliwości. Mądrością IoT są bazy danych, lokalne specjalistyczne, standaryzowane globalne bez ograniczeń w ich tworzeniu i dostępu, oraz sposobu korzystania z nich i wydobywania wiedzy, także nowej, metodami sztucznej inteligencji. Wymienione elementy składowe IoT rozwijają się technicznie ale podlegają innym ograniczeniom. Fundamentem dalszego rozwoju IoT wydaje się nie tylko technika ale także pokonywanie barier w obszarze społecznym. IoT, wprowadzając nowy poziom globalizacji, unifikacji i standaryzacji technicznej i społecznej, może prowadzić do zupełnie odmiennego od dzisiejszego rozumienia pojęcia produktu użytkowego, usługowego i funkcjonalnego. Będziemy wszędzie infrastrukturalnie jeszcze bardziej podobni niż dzisiaj. I nawet obserwowany obecnie chwilowy odwrót od globalizacji w kierunku regionalizacji tego nie zmieni. Technologia nie zna granic. W obszarze danych, ich wielkich ilości, i potencjalnie zawartej w nich wiedzy, globalizacja oznacza nieuchronnie wejście w świat poza technologiczny, ideologii, polityki, socjologii i psychologii, także kultury. Dobre dane, które nazywany strukturyzowanymi lub jasnymi, o wysokiej jakości i w wielkiej ilości, uzyskiwane ze źródeł takich jak IoT, już dzisiaj mogłyby potencjalnie przyspieszyć rozwiązanie wielu spraw gospodarczych, zrównoważonego rozwoju, związanych z żywnością, edukacją, energią, ubóstwem i zdrowiem. Dzisiaj posiadamy już sporo danych niestrukturyzowanych, nazywanych ciemnymi, tylko pośrednio przydatnych dla IoT. W wielu przypadkach trzeba zacząć zbierać dane od nowa, i IoT to robi już na masową skalę.

Powszechna i nieodwracalna internetyzacja naszej cywilizacji, a w szczególności Internet Przedmiotów nazywany inteligentną infrastrukturą, zasługuje bez wątpienia na swobodny esej mieszający nieco żartem a bardziej serio, nieco futurystyczny a bardziej osadzony w realnych możliwościach, takie aspekty jak: naukowe, techniczne i przemysłowe, ale także humanistyczne, socjologiczne i psychologiczne. Internetyzacja ‘dopadła’ nasze pokolenie i musimy sobie z nią poradzić, odnieść się do niej własnymi słowami, zobaczyć te słowa wydrukowane, usłyszeć je w czytaniu. Po to aby, jako współtwórcy, użytkownicy czy analitycy IoT, te skromne myśli móc porównać z ogromem słów i multimediów generowanych obecnie na ten temat co chwilę w postaci dziesiątków książek, tysięcy artykułów, not aplikacyjnych i instrukcji technicznych, także komentarzy bardziej popularnych. Nie zabranie głosu w tej sprawie i udokumentowanie go w postaci materialnej, nie dołożenie choćby skromnego wkładu intelektualnego, tak jakby pozbawia nas prawa do partycypacji w procesach przemiany i do krytyki. Internetyzacja jest nie tylko wielką przemianą ilościową, a jest przede wszystkim poważną przemianą jakościową, jak zmiana stanu skupienia materii. I to nie trywialną zmianą wody w lód, ale raczej w wysokotemperaturową plazmę. Jest całkowicie nową, jeszcze mało poznaną materią, tak jak plazma. Zaczęliśmy jak w filmie Alfreda Hitchcocka, niedoszłego inżyniera, mistrza suspensu, najpierw trzęsienie ziemi, a potem napięcie rośnie. Zadziwiający konsensus jest obserwowany od pewnego czasu wśród czołowych światowych specjalistów od inżynierii Internetu, sieci neuronalnych i sztucznej inteligencji. Panuje dość powszechna opinia, że od sztucznej samoświadomej superinteligencji, przewyższającej znacznie inteligencję człowieka, do której powstania przyczynia się walnie Internet, dzieli nas zaledwie kilka dziesięcioleci. Pesymiści mówią, że będzie to w ogóle ostatnie wielkie dzieło człowieka. Optymiści mówią, że jakoś utrzymamy kontrolę nad superinteligencją. Superinteligencja nie będzie osamotniona, będzie miała wówczas do dyspozycji podporządkowaną sobie inteligentną infrastrukturę, której skromne początki nazywamy dzisiaj Internetem Rzeczy czy Przedmiotów, i o którym piszemy w niniejszym eseju. IoT na pewnym, dostatecznie wysokim poziomie będzie zarządzany przez superinteligencję. Nie chcemy aby była ona zimna, inaczej mówiąc wyłącznie logiczna i bezrefleksyjna, czyli nieludzka. Dzisiaj nad superinteligencją maszynową pracują duże zespoły interdyscyplinarne w wielu czołowych laboratoriach świata – matematycy i informatycy, elektronicy, biofizycy, behawioryści i kognitywiści, fizjolodzy i neurolodzy, socjolodzy i psycholodzy, kulturoznawcy i logicy. Systemowo badane są i tworzone coraz bardziej antropomorfizowane składowe maszynowej superinteligencji emocjonalnej takie jak samoświadomość, rozpoznawanie własnych emocji i ich nazywanie, zdolność kierowania emocjami, zdolność wczuwania się w uczucia i potrzeby innych, łatwość nawiązywania i podtrzymywania kontaktów z innymi, pamięć asocjacyjna, i wiele innych. Badania te wspiera duży projekt europejski HBP dotyczący mózgu ludzkiego. Gdzie te cechy są fizycznie usadowione i realizowane, jeśli nie w mózgu człowieka składającym się w ok. 85% z wody? Podłożem fizycznym są oraz bardziej zaawansowane energooszczędne układy wielkiej skali integracji VLSI zawierające miliardy tranzystorów, posiadające wymiary bramek rzędu pojedynczych nanometrów, tysiące niezależnych procesorów programowalnych realizujące tryliony operacji na sekundę, działające niedeterministycznie w optymalizowanych architekturach neuromorficznych, dysponujące wielkimi zasobami pamięci i mocą obliczeniową, realizujące jednocześnie wiele scenariuszy działania, itp. Dopiero na takich podłożach możliwa jest implementacja dostatecznie złożonych algorytmów behawioralnych, emocjonalnych i kogniwistycznych. Konieczne jest zwrócenie uwagi, że projekty te napotykają silny opór pewnych części środowisk naukowych. Nawet jeśli wkrótce inteligencja maszynowa pokona ludzką, nie w sensie logicznym co okazało się proste, ale behawioralnym, świadomości i emocjonalnym to barierą może pozostać sprawność energetyczna. Choć i w tym zakresie prace postępują bardzo szybko nad tranzystorami kilkuatomowymi i jednoatomowymi, magnetycznymi pamięciami jednoatomowymi, nie mówiąc o postępach fotoniki i kwantowych procesorach optycznych. Jeśli dalej te argumenty są nieprzekonywujące to dlaczego komputery, wykorzystując zaawansowane algorytmy teorii gier, pokonały bezpowrotnie człowieka w szachy, warcaby, GO, a ostatnio maszyna DeepStack w najbardziej zaawansowaną wersję pokera teksański klincz? I to pokera wymagającego impasów i blefu? Poker, pokerem, ale DeepStack może pomóc lekarzom w diagnostyce i dobieraniu najbardziej skutecznych terapii. Dlaczego w niektórych krajach jak Japonia i Chiny zaczyna się zastępować ludzi pracujących w gospodarce oprogramowaniem AI i systemami IoT? I to w całkiem zaawansowanych funkcjach intelektualnych wymagających zdolności analitycznych i syntetycznych. Budujących swoją karierę zawodową młodych pracowników przygotowuje się tam już dzisiaj do współpracy, wręcz budowania zespołu, z inteligentnymi maszynami podejmującymi z człowiekiem zaawansowaną merytoryczną dyskusję (computer.org). Dlaczego kolejne kraje dopuszczają do ruchu drogowego autonomiczne samochody osobowe? Ostatnio zrobiła to Estonia, prawie nasz sąsiad. Dlaczego w wielu krajach opracowywane jest prawo dla osoby elektronicznej? Dlaczego dookoła nas kładzione są miliony kilometrów światłowodów, potrzebnych do budowy IoT i nowej gospodarki? Dlaczego w statystykach w tym obszarze nie jesteśmy w czołówce Europy? Będziemy zadawać delikatnie takie pytania.

Fizyka w roku 2116 to tylko częściowo zabawa znanego, popularnego czasopisma naukowego Amerykańskiego Towarzystwa Fizycznego „Physics Today”. Rozważaniom takim czasopismo poświęca ostatni zeszyt w roku 2016. Co dzisiaj przewidują fizycy i inżynierowie za sto lat? W astronomii jest to konstrukcja sieci super-teleskopów robotycznych, będących częścią naukowego IoT, orbitujących wokół Słońca z rozłożonymi zwierciadłami i o zdolności rozdzielczej pozwalającej obserwować powierzchnie planet w najbliższych systemach planetarnych tak jak widzimy z Ziemi Księżyc przy pomocy najlepszych obecnie teleskopów. To przewidywanie jest silnie zakotwiczone w ostatnich odkryciach planet podobnych do Ziemi i jest ono odwzorowaniem naszej nieprzezwyciężalnej tęsknoty za znalezieniem innego życia w kosmosie. W energetyce jest to opanowanie syntezy termojądrowej i wykorzystanie jej jako bezpiecznych źródeł nieskończonej energii. W fizyce cząstek elementarnych jest to zrozumienie natury czarnej energii i masy oraz konstrukcja następnego zderzacza po cernowskim LHC i potencjalne odkrycie dalszej unifikacji sił elementarnych oraz kwantyzacji grawitacji i przestrzeni, a przez to umożliwienie dalekich podróży kosmicznych. W sztucznej inteligencji jest to, już wspomniane powyżej, pokonanie bariery samo-świadomości i budowa inteligencji emocjonalnej maszyn. W przestrzeni bezpieczeństwa, wolności, jakości i stylu życia są to kompletne zmiany otoczenia człowieka związane z łatwością gromadzenia przez sieć globalną ogromnych ilości danych i wykorzystanie tych danych przez społeczeństwa do budowy inteligentnej infrastruktury mogącej polepszyć i znacznie zmienić nasze życie.

Podobne rozważania dotyczące czasu przyszłego techniki prowadzi raz do roku, w zeszycie styczniowym, jedno z najbardziej wpływowych czasopism technicznych IEEE Spectrum. W osiągnięciach

naukowo-technicznych ubiegłego roku poszukiwane są potencjalne korzenie rozwiązań przyszłości. Nic dziwnego, że już od kilku lat duża część z tych szerzej omawianych osiągnięć dotyczy bezpośrednio lub pośrednio budowy inteligentnej infrastruktury cywilizacyjnej, czyli mówiąc językiem popularnym Internetu Przedmiotów. Nazwa ta przyjęła się zarówno w literaturze naukowej, popularnej jak i w języku potocznym. Badania nad Internetem Przedmiotów są prowadzone przez wiele dziedzin nauki jak: matematyczne, ekonomiczne, humanistyczne, medyczne, prawne, oraz techniczne. W wielu dyscyplinach nauki Internet Przedmiotów wyznacza nowe kierunki badawcze jak np. w: filozofii, prawie, ekonomii, medycynie, organizacji i zarządzaniu, pedagogice, psychologii, socjologii, informatyce, architekturze, telekomunikacji, elektronice i technikach informacyjnych, i innych. Internet Przedmiotów tworzy w niektórych z tych dyscyplin nowe specjalności naukowe jak np. współprojektowanie i integracja oprogramowania i infrastruktury, kognitywistyka maszynowa, głębokie uczenie maszynowe, inżynieria Internetu Przedmiotów czy na końcu usługowy i przemysłowy Internet Przedmiotów. Ktoś zapyta, co ma do tego filozofia? Antycypowana potęga przyszłej inteligencji infrastrukturalnej tworzącej potencjalnie nowe ramy cywilizacyjne, także w obszarze wirtualizacji, każe niektórym filozofom, psychologom i socjologom, a także i nam, inaczej spojrzeć na nasz świat i zadać od nowa wiele pytań fundamentalnych, ontologicznych, bytowych, a w tym pytanie czy nie żyjemy w matriksie. Od nowa zadajemy pytanie o istotę rzeczy, tym razem wspierając się coraz szybciej gromadzonymi dowodami o subtelnej istocie naszej świadomości i potencjalnej możliwości jej odtworzenia maszynowego, o relatywnie prostym oprogramowaniu naszego DNA, jeśli dysponuje się komputerem kwantowym. O wielu dziwnych pozostałościach w naszym DNA, jakby nie do końca trafionych próbach pisania oprogramowania. Kolejna bariera na drodze do komputera kwantowego została ostatnio pokonana. Google i NASA instaluje w ośrodku badawczym w Ames prototyp takiego komputera D-Wave działający na 2000 qbitach. Komputer stanowi wyposażenie laboratorium badawczego nad kwantowym rozwiązaniem sztucznej inteligencji. Samo-świadoma sztuczna inteligencja i pełna informacja o naszym lokalnym świecie ludzkim gromadzona w sposób standaryzowany, konsekwentnie i systematycznie przez pewien czas może prowadzić, do pełnej wiedzy lokalnej, a przez to do tego że człowiek stanie się niepotrzebny do wytwarzania czegokolwiek. Chyba nie zanikniemy, pozostanie wszakże emocja, myśl ulotna, wyobraźnia, przyjaźń, miłość, idea, także w ostateczności dolce far niente. Pełna (prawie) wiedza lokalna, i potencjalna świadomość niewoli nic-nie-robienia prawdopodobnie nie służy dobrostanowi i szczęściu człowieka. Parafrazując Szekspira, być czy nie być częścią nadchodzącej, coraz bardziej wirtualizującej się rzeczywistości, udźwigniemy, czy nie udźwigniemy ten nieznany ciężar, oto są pytania?

Przed przejściem do dalszych rozważań, zakładając że cały czas jesteśmy jeszcze na początku i nie poruszyliśmy kwestii zasadniczych, konieczne wydaje się poczynienie pewnych założeń, mających na celu nie narażenie czytelnika na zniechęcenie i zawód przez potraktowanie tekstu jako swobodnego eseju futurystycznego. Przede wszystkim nadużywane będzie tutaj słowo inteligencja, w przenośni, w różnych znaczeniach zależnych od kontekstu, odległych od znaczenia inteligencja ludzka. Trzeba byłoby ciągle używać określeń sztuczna czyli AI, neuronalna, obliczeniowa, elementowa, maszynowa, wirtualna, chmurowa i mglista, brzegowa i centralna, głęboka i emocjonalna. Ponadto trzeba byłoby dodać do tego terminu opracowane ostatnio 23 szlachetne i wydaje się bardzo ważne Reguły AI z Asilomar, w fundamentalny sposób dotykające rozwoju IoT i robotyki, promowane przez Instytut Przyszłości Życia FLI – The Future of Life Institute (futureoflife.org). Nadmierne akcentowanie w tekście roli IoT w przyszłości jest być może uzasadnione obecnym szerokim zainteresowaniem nauki tym tematem, w tym mediów społecznościowych, ale nie wykluczone że i modą. Wielkie europejskie, japońskie i amerykańskie inicjatywy naukowo – przemysłowe, miliardowe w skali finansowej, dotyczące sztucznej inteligencji w IoT i cyfryzacji gospodarki, konsorcja społecznościowe i projekty takie jak np. Konsorcjum Internetu Przemysłowego IIC, Przemysł 4.0 czy OpenFog Computing, a także SMAC, nie są jednak przypadkiem. Opis niektórych istniejących i potencjalnych atrybutów IoT będzie dość często powtarzany w różnych kontekstach, w celu pokazania różnorodności rozwoju tego nowego zjawiska cywilizacyjnego. Będziemy starali się ograniczać rozważania do nauk technicznych, wychodząc poza ten obszar jedynie w niezbędnych przypadkach koniecznych do zachowania ciągłości wywodu. Nie będzie to jednak łatwe. Mimo znacznego podłoża technicznego potrzebnego do budowy systemu IoT sprawnie i funkcjonalnie sprzężonego z infrastrukturą cywilizacyjną, znaczenie technicznej części IoT będzie malało na rzecz przewidywanego w przyszłości bardzo silnego oddziaływania gospodarczego i społecznego, także kulturowego. W przyszłości IoT, wówczas zapewne inaczej nazywany, będzie bardziej zjawiskiem społecznym i cywilizacyjnym niż technicznym. Dzisiaj jednak Internet Przedmiotów rodzi się na naszych oczach, budowany z różnorodnych cegiełek technicznych, w interdyscyplinarnych zespołach naukowych, inspirowany marzeniami ale też obawami uczonych i użytkowników. Ile z tych marzeń badawczych i laboratoryjnych zostanie zaakceptowanych, tego nie wiemy. Zapewne sporo nie zostanie. Na razie nie obserwujemy jeszcze wielkiego, naprawdę zasadniczego przełomu w zakresie oddania władzy Internetowi Przedmiotów. A może będzie to zmiana wolniejsza, ewolucyjna. Należy więc do niektórych przedstawionych tutaj marzeń ale i obaw podchodzić z rezerwą. IoT w połączeniu ze sztuczną inteligencją buduje rzeczywistość, cyfrową infrastrukturę cywilizacyjną a w niej musi znaleźć się analogowy człowiek, cyfrowy człowiek i społeczeństwo. Zadajemy więcej pytań, niż udzielamy odpowiedzi. Jeśli jednak potrafimy dzisiaj już zadać niektóre z tych pytań, choćby brzmiących absurdalnie, choćby nie mających obecnie żadnej recepty technologicznej, oznacza to że jest nietrywialna przyczyna. Transhumanizm i przewaga intelektualna maszyn budzi wielkie obawy, a to są prawdopodobne atrybuty przyszłego IoT, jeśli wymknie się spod kontroli, podda absolutnej władzy pieniądza i nauki bez sumienia. Pytań nie zadajemy w pewnych obszarach, nie zdając sobie sprawę że istnieją, a nie ma wątpliwości że istnieją. Niektóre z tych obszarów, także IoT, są finansowane przez miliarderów ‘filantropów’ którzy w nauce mogą zrobić dzisiaj więcej niż całe kraje. Ograniczamy się tutaj do zasygnalizowania wielu dużych, fundamentalnych obszarów IoT, nie wchodząc jednak w żadnym z nich zbyt głęboko. Wyjątkiem będzie kilka szczegółowych przykładów i ciekawostek charakteryzujących pewne kierunki rozwoju. Prawie każdy z tych dużych obszarów np. inteligentne miasto czy cyberbezpieczeństwo IoT jest dzisiaj przedmiotem szybkiego rozwoju i głębszych analiz, bardzo często dostępnych publicznie w postaci szerokich opracowań społecznościowych. Opracowania takie są także dostępne w wersjach popularnych. W ten sposób wszyscy wszystko wiedzą natychmiast z Internetu. Podobnie jest z niniejszym esejem. Nic tutaj nowego. Można sobie samemu wszystko łatwo znaleźć w sieci i sprawdzić. Tutaj zbieramy tylko to razem, opatrując czasami bardziej obiektywnym, częściej subiektywnym komentarzem. Jaskrawym dowodem na głęboką i nieodwracalną penetrację technologii ICT i IoT w życie społeczne, rynki, handel, marketing, itp. jest sytuacja największych targów komputerowych na świecie, trzydziestoletniego hanowerskiego CeBitu. Nie ma tam żadnych nowości. Rynkowi giganci prezentują nowości w mediach społecznościowych. Jest to miłe dla biznesu spotkanie towarzyskie, jednak nadal organizowane z wielkim rozmachem. Jeszcze z niektórymi nowościami konsumenckimi, w tym obecnie w dużej mierze IoT, trzyma się pięćdziesięcioletnia wystawa i konferencja Stowarzyszenia Technologii Konsumenckich CES w Las Vegas.

Rozwój techniczny IoT, jego przemiany ilościowe w bogatą i zróżnicowaną jakość, oraz sprzężenie techniki IoT z infrastrukturą i przestrzenią społeczną, z nowymi usługami, otwierają nurt dyskusji dotyczący wolności człowieka. Pomiędzy wyraźnie obecnymi w tej dyskusji dwoma biegunami, że IoT znacznie ograniczy i bardzo rozszerzy wolność rozciąga się olbrzymie pole nowej nauki. Nieco trywializując, musimy sobie odpowiedzieć na wiele pytań, na przykład czy jesteśmy gotowi oddać część swojej władzy decyzyjnej dotyczącej odżywiania naszej ‘inteligentnej’ lodówce, która po pewnym czasie nie tylko pozna nasze zwyczaje, ale może popaść w monopolistyczną zależność od jakiegoś jeszcze bardziej inteligentnego dostawcy. Na lodówkę i inny sprzęt AGD klasy IoT będziemy powoływać się kilkukrotnie. Mimo tych niepewności dotyczących akceptacji rezygnacji z naszej wolności wyboru, a może przeniesienia tej wolności na inny poziom, trwają chyba najintensywniejsze (oprócz ‘obronności’) prace badawcze nad rozwojem IoT usługowego specjalizowanego w bezpośredniej i pośredniej obsłudze człowieka. IoT według tej koncepcji ma stać się ‘opiekuńczy’ wobec człowieka. Najaktywniejsi twórcy i użytkownicy IoT werbalizują odważnie swoje oczekiwania. Wcale nie najodważniejsze z nich to ścisłe sprzęgnięcie człowieka z Internetem Przedmiotów, zarówno fizyczne, kiedyś transhumanistyczne, jak i obecnie wirtualne, zanurzeniowe przy pomocy jego bliźniaka cyfrowego, mojego pracowitego bio-bota, mojego wirtualnego bionicznego Anioła Stróża. Otaczające tematykę IoT ze wszystkich stron niebezpieczeństwo szybkiego popadnięcia w obszar sci-fi może być zmniejszone jedynie poprzez słabsze lub silniejsze zakotwiczenie każdego

opisanego przypadku w realnych współczesnych badaniach naukowych w wielu dziedzinach, dyscyplinach i specjalnościach naukowych wymienionych powyżej. Na wszelki wypadek z podanymi, na ile to możliwe, ścisłymi odnośnikami literaturowymi do źródeł badawczych i przemysłowych. Do dalszych losów IoT, jednak zakotwiczonych w dzisiejszych badaniach, konieczny będzie powrót rozważając wirtualizację i cyberbezpieczeństwo i inne artrybuty i pola zastosowań. Abstrahując teraz od nieco dalszej przyszłości IoT, którą intencjonalnie rozpoczęliśmy rozważania, wracamy do dnia dzisiejszego. Dla IoT rozpoczynającego dzisiaj budowę złożonej inteligencji infrastrukturalnej, mamy spróbować poruszyć kilka prostszych zagadnień raczej dotyczących jutra, co najwyżej pojutrza, niż nadchodzących dziesięcioleci. Co to jest tak naprawdę IoT z technicznego punktu widzenia? Jakie są jego składniki elementarne? Jak nauka we współpracy z przemysłem transformuje specyficzny rodzaj badawczego IoT, nazywanego RIoT, w IoT usługowy, komercyjny CoIT, przemysłowy, nazywany IIoT. A wszystkie te rodzaje IoT powinny posiadać atrybut kognitywny IoT^{C}.

Bogactwo źródeł drukowanych i internetowych o IoT (iot.ieee.org), (theinternetofthings.eu), (thethings.io), pierwotnych (resiot.io) i wtórnych (iotjournal.com), profesjonalnych (aws.amazon.com/iot), (evrythng.com) i popularnych (iotworldnews.com), świadczy o gigantycznym zainteresowaniu nauki, techniki, przemysłu, gospodarki i społeczeństwa tą tematyką. Obecnie główna literatura dotycząca wszystkich aspektów IoT to różnej wagi źródła internetowe (internet-of-things-research.eu), (iotweekslynews.com), (iottedchnews.com), (iotnewsnetwork.com), (iotbusinessnews), (iot-today.com), (iot-now.com), społecznościowe (Prpl 2016), (iofthings.org), (iotcentral.io), (internetofthingsagenda.techtarget.com), książkowe popularne (Sterling 2014), (Li 2015), (Miller 2015), i naukowo-techniczne (Alam 2017), (Romaniuk 2001), (Vermesan 2016), firmowe (Cisco, IBM, Intel, Amazon), (Rossman 2016), (Womack 2016), raporty techniczne (Eclipse 2016), (IIConsortium 206), standardy (IIConsortium 2015), materiały konferencyjne (Tervonen 2015), (Floerkemeister 2008), książki o różnym poziomie – wstępnym (Pfister 2011), (Etter 2017), ogólnym (Miessler 2017), (Mukhopadhayay 2014), (Pan 2016), (DaCosta 2013), praktycznym (Kurniawan 2016), (Chen M 2017), (Achwartz 2016), i zaawansowanym (Behman 2015), dotyczące obecnych rozwiązań (Chou 2016), (Rayes 2016) i przyszłości (Acharjya 2017), (Prasad 2016), (Batalla 2016), (Burakowski 2012), (Jamthe 2016), przeglądowe (Anissimov 2015), techniczno-praktyczne (Bagha 2014), (Rogers 2017), (Chin 2015), e-booki (BBVA 2016), (Nagpure 2016). Są ich tysiące, dziesiątki tysięcy, zmieniające się z dnia na dzień. Niniejsze opracowanie bazuje zarówno na wnikliwej lekturze setek takich dokumentów, przeglądnięciu kolejnych setek, ale także na pracach własnych w obszarze sprzętu, oprogramowania i architektury systemów IoT prowadzonych na terenie macierzystej uczelni i dla wielkich eksperymentów badawczych w CERN, GSI, JET, itp. Linki do wielu z wykorzystywanych fragmentarycznie grup dokumentów można łatwo znaleźć samodzielnie. Materiały z tych wielu rozmaitych źródeł są prezentowane tutaj raczej nie indywidualnie a syntetycznie w poszukiwaniu tendencji rozwojowych nauki (Guerrieri 2016), ewentualnego transferu do przemysłu (Gilchrist 2016), i potencjalnych skutków społecznych i gospodarczych (Slama 2000), (Smart 2014), (Vermesan 2014, 2015, 2016). Jako twardą bibliografię od której być może warto rozpocząć studia na temat technicznych aspektów IoT w obszarze nauka – przemysł podajemy kilkadziesiąt pionierskich książek rozpoczynających lawinowo tą tematykę, np. (Buyya 2016), (Fortino 2014), (Greengard 2015), (Liow 2017), oraz aktualne kluczowe noty techniczne dużych organizacji tworzących standardy Internetu Przedmiotów IoT oraz jego wersji badawczej RIoT, konsumenckiej CIoT i przemysłowej IIoT (Santana 2013), (IBM 2015). Ze skrótami IoT trzeba uważać, stabilizują się częściej używane, powstają ciągle nowe. Na przykład skrót CIoT lub IoT^{C} jest także używany w odniesieniu do przyszłościowego kognitywnego IoT, a także do kolaboratywnego IoT i chmurowego IoT. Techniczne zagadnienia badawcze IoT, z natury pisane językiem specjalistycznym dla danej dziedziny nauki, stąd dość hermetycznym, są w literaturze światowej rozproszone w wielu czasopismach naukowych dotyczących sztucznej inteligencji, automatyki i robotyki, telekomunikacji, systemów czujnikowych, a także powstających czasopismach dedykowanych prawie wyłącznie tej tematyce (Mach 2017), (Al-Fuquaha 2015). Takim czasopismem dostępnym w bazie danych IEEE eXplore, jest IEEE IoT Journal łączący Stowarzyszenia IEEE Społecznego Wpływu Technologii, Niezawodności, Telekomunikacji, Inżynierii Komputerowej, Elektroniki Konsumpcyjnej, Zastosowań Przemysłowych, Czujników i Przetwarzania Sygnałów (Stankovic 2014) (iot-journal.weebly.com). W tak szybko rozwijającej się dziedzinie książki o IoT są wydawane z pewnym opóźnieniem wobec treści publikowanych w artykułach naukowych w czasopismach internetowych, mimo szybkiego wzrostu popularności e-booków. Książki o IoT dotyczą przykładowo: tematyki biznesowej (Adams 2016), (Behman 2015), (Jackson 2016), (Jamthe 2015), zmiany modeli biznesowych i zaufania (Kranz 2016), (Smith 2017), (Thampi 2014), analityki biznesowej (Covington 2015), (Smith 2016), finansów (Chishti 2016), (Mougayar 2016), (Skinner 2016), (Tapscott 2015), psychologicznej (Aiken 2016), (Atrill 2015), (Connoly 2016), sztucznej inteligencji (Armstrong 2016), (Kellmereit 2013), superinteligencji (Bostron 2014), (Berglass 2015), (Barrat 2013), (Chace 2015), zdrowia (Bhatt 2017), przyszłości człowieka i cyfrowej generacji ludzi (Brain 2015), (Palfrey 2013), (Volkman 2016), cyberbezpieczeństwa (Brooks 2017), (Elbas 2017), (Etter 2016), (Chmielecka 2017), (Gilchrist 2017), (Russell 2016), prywatności (Hu 2016), (Li 2017), architektury (Ashgar 2016), (Bassi 2013), (Uckelmann 2011), protokołów i algorytmów (Perera 2014), (Delikato 2013), projektowania IoT (Case 2015), (Chou 2016), (Rowland 2015), IoT przemysłowego i kognitywnego (Wu 2014), (Xu 2014), (Mcaulay 2000), sieci i wirtualizacji (Liyanage 2015), (Pujolle 2015), ekonomii i gospodarki, przedsiębiorstw (Balani 2016), dydaktyki i kształcenia (Waher 2015), inteligentnych miast (Angelakis 2017), (Foth 2015), (Seta 2016), inteligentnego domu (Dennis 2015), obliczeń chmurowych i mgłowych (Erl 2013), (Markakis 2017), (DiFatta 2015), (Rupelia 2016), interoperacyjności (Zarko 2016), systemu 5G (Marvomoustakias 2016), (Rodriguez 2015), (Sarver 2017), czujników dla IoT (Fraden 2016), oprogramowania (Guinard 2016), (Faihead 2016), wielkich zbiorów danych (Jaokar 2015), (Stackiwiak 2015), transformacji pomiędzy technologiami IoT i M2M (Holler 2014), (Chen S 2017), mikroprocesorów i mikrosystemów dla IoT (Jayakumar 2017), (Kuhnel 2015), (Javed 2014), (Shovic 2016), gospodarki zasobami IoT (Delikato 2017), oczekującego nas potencjalnie konfliktu IoT maszyna – człowiek (Leonhard 2016), (Ford 2015), (DelMonte 2016), inteligentnych ubrań (Hartman 2014), (Olsson 2012), (Pailes-Friedman 2016), (Sazonov 2014), konwersji usług (Familiar 2016), oraz przykładów zastosowania (McEvan 2014), (Darnell 2016). Czasopisma naukowo-techniczne, działające w wymienionych dziedzinach współtworzących IoT, stosujące popularny standard 'najpierw na sieci', recenzują i publikują prace nawet w dwa tygodnie. Jeszcze inna sytuacja dotyczy opracowywanych przez duże zespoły standardów technicznych IoT dotyczących ogólnych zagadnień architektury IoT i IIoT i zagadnień specjalistycznych dla konkretnych zastosowań w gospodarce. Na ogół dojrzewają one kilka lat i publikowane są rozwiązania częściowe w celach otwartej konsultacji przez użytkowników przemysłowych i społecznościowych. Dostępne są także, ale odpłatnie, liczne pogłębione analizy firmowe dotyczące poszczególnych sektorów IoT jak ekosystemu IoT, nisko-zasobowej sieci WAN dla IoT, brzegowego przetwarzania informacji w IoT, itp. Jedno z takich bardzo obszernych płatnych opracowań o transferze IoT między nauką a przemysłem dla wielu sektorów gospodarczych jest dostępne z firmy BI Intelligence (businessinsider.com). Język not technicznych i standardów, szczególnie dla IIoT, jest najbardziej hermetyczny. Dotyczy na przykład optymalizowanych i standaryzowanych, wysoce niezawodnych protokołów dla oszczędnych informacyjnie magistrali IIoT brzegowego, a także aplikacyjnie zorientowanych topologii mini sieci proksymalnych, minimalnie latencyjnych, oszczędnych pod względem krytycznych zasobów, np. energii. W rozwiązaniach biznesowych optymalizowanych sieci dostępowych IoT i IIoT standardy dotyczą np. wpływu agresywności i asertywności węzła na efektywność ekonomiczną zastosowanego w środowisku firmowym systemu. Nie polecamy lektury takich tekstów czytelnikom niniejszego eseju, a szczególnie managerom i ekonomistom, w celu wzbogacenia swojej wiedzy o IoT. Natomiast ciekawym źródłem przystępnych lektur o bieżących uwarunkowaniach rozwoju technicznego, ekonomicznego, gospodarczego i społecznego IoT stają się powstające czasopisma omawiające nowości, jak np. Magazyn IoT News (iottechnews.com), BusinessIntelligence.com, i inne.

Obszar kontaktów pomiędzy firmą a klientem, firmą a rynkiem bardzo silnie się IoT-yzuje. Obszar ten jest przedmiotem standaryzacji dla rozwiązań technicznych z oczywistych względów ekonomicznych i łatwości użytkowania np. korzystając ze znanego każdemu Androida. Podłoże techniczne IoT, nie widoczne bezpośrednio dla użytkownika, musi jednak pozostać w gestii inżynierów i informatyków. Użytkownicy oceniają i ewentualnie akceptują lub nie funkcjonalności aplikacji. Takie sprzężenie zwrotne działa dość dobrze i normy

podlegają ciągłej ewolucji. To znaczy są zamrażane na jakiś czas umożliwiając przemysłowi produkcję sprzętu i oprogramowania IoT a następnie są zmieniane skokowo na następną wersję, potencjalnie choć nie zawsze, z kompatybilnością wsteczną. Okres gwałtownego rozwoju technicznego jaki obserwujemy w IoT, i w związku z tym przyspieszonego tempa opracowywanych norm przemysłowych, tej kompatybilności w zasadzie dzisiaj nie gwarantuje. Chcąc korzystać z najnowszych generacji rozwiązań sprzętowych i programistycznych IoT musimy ciągle inwestować indywidualnie lub firmowo. IoT jest kosztownym obszarem, ale potencjalnie bardzo atrakcyjnym. Co tu dużo mówić, dla biznesu staje się standardem, wręcz nową uniwersalną wielowarstwową platformą działania, nowym środowiskiem działania i wspólnym uniwersalnym językiem porozumienia. Jeśli sprawa rozwoju i szerokiej penetracji przez IoT naszej cywilizacji jest aż tak skomplikowana i ważna, to spróbujmy najpierw nieco dokładniej odpowiedzieć na pytanie co to dokładnie jest IoT z technicznego punktu widzenia

Definicje techniczne IoT

O IoT można powiedzieć że jego budowa i funkcjonalność prowadzi od wielkiej masy różnorodnych drobiazgów, o wąskich specjalnościach, do coraz większych systemów inteligentnych i autonomicznych (Miessler 2017). Dosłownie, Internet Przedmiotów rozpoczyna się od drobiazgów. Inteligentne czujniki i sterowniki zbierają zygnały i obsługują małe lub większe urządzenia nadając im dodatkowe funkcjonalności, przydatne bezpośrednio dla tego urządzenia lub, jeśli połączone w sieć, przydatne dla większych infrastruktur funkcjonalnych. Inteligencja, jeśli jest potrzebna i akceptowalna, wyposaża niektóre z takich urządzeń w autonomię dalej zwiększającą funkcjonalność. Inaczej mówiąc IoT, w najprostszym ujęciu strukturalnym z punktu widzenia człowieka to liczne wejścia i wyjścia, dane, warstwa logiczna i wizualizacja. IoT jest jednak znacznie bardziej skomplikowany niż czujniki i sterowniki, akwizycja, transmisja, przetwarzanie, analiza, wykorzystanie i wizualizacja danych. IoT jest platformą tworzenia nowej, ruchomej, i ciągle zmiennej rzeczywistości społecznej, gospodarczej i cywilizacyjnej (Jamthe 2016). IoT dodaje do sieci web dodatkowy trzeci, pionowy wymiar, segmentuje i komplikuje sieć. Można powiedzieć, że w epoce przed IoT sieć web była ogromną strukturą płaską, boiskiem z wieloma jednoczesnymi zawodami, gdzie głównie sędziował Google. IoT systematycznie zaludnia Internet bytami autonomicznymi, obdarzanymi coraz większą inteligencją. Kiedyś taką przestrzeń być może nazwiemy także cywilizacją. IoT podlega szybkiemu różnicowaniu. Mówimy, że nie ma jednego IoT. Wymieniane są co najmniej dwa różniące się znacznie od siebie IoT, konsumencki CIoT oraz przemysłowy IIoT, czasami opisywane kolorami IoT zielony i IoT brązowy. Zielony to budowa struktur od początku. Brązowy to adaptacja, dostosowanie i przebudowa. CIoT to IoT dotykowy, rynkowy, masowy, medialny, usługowy, bliski człowieka. IIoT to rozwiązania indywidualne, masywna komunikacja międzymaszynowa M2M, automatyka, inteligencja i niezawodność przemysłowa, także infrastruktura cywilizacyjna.

IoT można zdefiniować z technicznego punktu widzenia na kilka odmiennych sposobów. Definicje takie uwypuklają kluczowe składowe IoT układające się w pewną całość nazywaną architekturą działającą, jak się mówi na platformie lub w ekosystemie (Uckelman 2011), (Zhang 2015). Każda z tych składowych IoT posiada pewną autonomię w sensie mniej lub bardziej widocznych granic domenowych między nimi, różnic zastosowanych technologii, rodzajów technicznych interfejsów sprzętowo – programistycznych i komunikacyjnych. To właśnie istnienie tych granic pozwala jeszcze dzisiaj na spoglądnięcie na IoT z kilku kierunków. W ramach takich granic nauki techniczne pracują nad rozwojem różnych atrybutów IoT. Być może w przyszłości te granice strukturalne będą zanikać wraz z postępem techniki. Spotyka się także definicje pozatechniczne lub hybrydowe, bardziej ogólne, próbujące łączyć w logiczną całość wiele odmiennych charakterystyk IoT. Nikt jeszcze dokładnie nie wie, mimo coraz szerszych prac w kierunku e-społeczeństwa, co oznaczają coraz częściej używane w naukowej literaturze technicznej i humanistycznej a także biznesowej, bardzo ogólne terminy np. Społeczeństwo v.4, Cywilizacja v.3 lub wyższa, Biznes v.4, Przemysł, v.4, gdzie ważnym elementem jest np. IoT v.2, lub IoT v.2.5. Gdzieniegdzie, szczególnie w podejściu ‘rewolucyjnym’ mówi się że budowana obecnie kategoria Przemysł jest wersji 4 po rewolucjach parowej, elektrycznej, obecnej internetowej i nadchodzącej związanej ze sztuczną inteligencją (Gilhrist 2016). Z tymi terminami i ich wersjami trzeba jednak uważać, bowiem e-biznes zawłaszczył powyższe nazwy dla gier komputerowych i rozwijanej dla nich wirtualnej rzeczywistości z coraz sprawniejszymi i bardziej realistycznymi efektami zanurzenia cyfrowego i wspomaganej rzeczywistości. Poszukując mimo wszystko wspólnego mianownika pomiędzy wydawałoby się odległymi światami IoT i gier komputerowych mamy np. wirtualizację rzeczywistości i doskonalenie bio-botów. Techniki jeszcze niezbyt często wykorzystywane w IoT, ale wszystko przed nami. Jednym z badanych kierunków rozwojowych IoT jest jego ‘gamizacja’, już dziś aplikowana z sukcesem w niektórych systemach biznesowych IoT. Szczególnie w kontaktach z klientami.Tego terminu chyba nie trzeba tłumaczyć, a skutków nie da się dokładnie przewidzieć, oprócz tego że takie ujęcie niewątpliwie przyciągnie młodzież, podlegającą na naszych oczach transformacji w pokolenie cyfrowe, pokolenie IoT i Socjalnego Internetu Wiedzy. Dopiero na zastanych i przyjętych jako oczywiste funkcjonalnościach IoT (które właśnie teraz projektujemy, testujemy i nieśmiało prowadzamy) to następne pokolenie cyfrowe będzie w stanie zbudować w przyszłości, za swoich czasów, praktyczne i akceptowalne generacje funkcjonalności. Gamizacja jest początkiem wchodzenia w IoT rzeczywistości wirtualnej. Nasze, na szczęście krótkie, rozważania o pokolenie czy dwa wprzód dotyczące IoT mają charakter wielce niepewnej transakcji ‘fumum vendere’.

Definicja źródłowo- i sygnałowo-centryczna podkreśla rolę źródeł sygnałów i danych i stawia je na pierwszym miejscu. W tym ujęciu można powiedzieć, że istotą IoT są sygnały i dane lokalne, ich zdobywanie i przetwarzanie w informacje, w taki sposób aby wykorzystywać je do kontroli urządzań i przez to tworzenia lokalnej inteligentnej infrastruktury cywilizacyjnej. Na tyle inteligentnej, aby umożliwiać optymalizację wybranych ważnych procesów przede wszystkim lokalnie, np. monitoringu bieżących zadań, pomiaru parametrów, kontroli procesów produkcyjnych, działania lokalnych firm, zużycia energii, bezpieczeństwa, ciągłego zapewnienia krytycznych funkcjonalności, itp. Słowo inteligencja jest tutaj oczywiście jeszcze w dniu dzisiejszym nieco, a w niektórych przypadkach nawet bardzo, nadużywane. Fundamentem działania IoT będzie masowe pobieranie lokalnych danych, ewoluujące zapewne w kierunku jakiejś wybiórczości i optymalizacji tego pobierania. Źródeł danych będzie coraz więcej. Już dzisiaj obserwujemy taki wzrost. Wkrótce zmieni się w lawinowy. Znacznie zwiększy się różnorodność źródeł danych i metod pobierania od nich informacji. IoT będzie zawierać gigantyczną liczbę źródeł generujących niewielkie ilości danych, wśród których duża część będzie źródłami śpiącymi, budzonymi w razie potrzeby. Niewielkie ilości danych generują proste czujniki pojedynczych wielkości wolnozmiennych. Takich źródeł będzie najwięcej. Postęp w obszarze technologii czujników został znacznie przyspieszony wskutek znacznego zapotrzebowywania ilościowego i jakościowego ze strony IoT (Faden 2016). Opracowywane są dla IoT inteligentne mikroczujniki pojedynczej wielkości, które korzystając z technologii głębokiego usypiania, potrzebują mocy na poziomie pikowatów do poprawnego działania. To stanowi zupełny przełom technologiczny wobec sytuacji sprzed kilku lat. Znaczne strumienie danych generują źródła wideo, a w przemyśle np. systemy pomiarowo-kontrolne szybkich procesów on-line w czasie rzeczywistym. Masowe dane zawierają informacje i następnie wiedzę do odkrycia na poziomie lokalnym ale też na poziomach wyższych. Te dane są wokół nas, docierają z wielu kierunków i posiadają bardzo różnorodny charakter (Stackowiak 2015). Albo nie były zbierane, albo były ale w sposób niestandaryzowany. Standaryzacja już posiadanych danych ze źródeł lokalnych czasami nie jest możliwa z powodu braku krytycznych elementów w takich danych, np. czasu, miejsca, metod i warunków akwizycji. Takie dane mają znacznie mniejszą wartość. Dane standaryzowane, tworzone z sygnałów, z różnych źródeł, pełne, o wysokiej jakości są bardzo cenne. Będą stanowić fundament IoT. Na razie tych dostarczających dane czujników jest jeszcze relatywnie niewiele, mimo iż mówimy o miliardach. To w skali świata niewiele, gdyż decyduje nie liczba a gęstość, ale ta liczba gwałtownie rośnie. Uważa się, że jeśli gęstość rozkładu czujników i sterowników, oraz innych źródeł, w tym mobilnych, wzrośnie znacznie np. dziesięciokrotnie, może stukrotnie, wymagając rozwiązania problemu komunikacji M2M w bardzo gęstym środowisku komunikacyjnym (Chen 2017), to dopiero wówczas może dojść do przemiany jakościowej IoT, otwierając przestrzenie techniczną, społeczną i cywilizacyjną dla dzisiaj zupełnie nieprzewidywalnych usług.

Istotą źródłowo-centrycznego ujęcia IoT jest tzw. informacja brzegowa oraz obliczenia brzegowe, w literaturze za Cisco, określane terminem ‘fog computing’ (Narvomoustakias 2017). Mgła jest rozszerzeniem chmury w obszar brzegu IoT, czyli przedmiotów. Miejsce generacji sygnałów pomiarowych i ich akwizycji w postaci danych, oraz sposób tej akwizycji i wstępnego przetwarzania sygnałów analogowych na dane brzegowe nazywamy brzegiem IoT. Brzeg IoT będzie strukturą bardzo rozbudowaną. Mówi się wręcz o strukturach frak-

talnych. Jeśli brzeg IoT moglibyśmy mierzyć długością, i miało by to sens np. logistyczny, finansowy czy funkcjonalny, to będzie on miał miliony kilometrów. Brzeg IoT jest także mobilny, co dodaje się znacznie do jego długości i funkcjonalności. Brzeg IoT jest coraz bardziej obciążany zwiększającą się liczbą funkcji, w tym masywnymi połączeniami z czujnikami, oraz obliczeniami brzegowymi. Prowadzone są zawansowane prace nad technikami odciążenia brzegu i minimalno -latencyjnej delegacji zadań obliczeniowych do chmury (Mach 2017). Poznawanie i świadomość kontekstu i zawartości generowanej informacji brzegowej ułatwia jej wstępną lokalną klasyfikację i zmniejsza obciążenie obliczeniowe brzegu IoT (Perera 2014), (Tervonen 2015). Brzeg to jedyna struktura IoT nie podlegająca większej formie centralizacji, a raczej odwrotnie podlegająca znacznej dyssypacji. Podejście źródło-centryczne do IoT nie tyle charakteryzuje się globalizacją ile znacznie bardziej lokalizacją i rozproszeniem, oraz różnorodnością. Lokalna sieć źródeł danych dostarcza wartościowych informacji zawierających wiedzę mogącą uczynić lokalne miejsce bardziej funkcjonalnym, z jednej strony bardziej wyspecjalizowanym a z drugiej przeciwstawnie uniwersalnym, nawet w pewnym sensie samowystarczalnym. To dopiero podejście globalne do IoT uczyniło z ujęcia źródło-centrycznego brzeg większych struktur, poprzez integrację wielu struktur lokalnych, co zresztą było do przewidzenia wskutek rozwoju sieci Internet. IoT źródłowo-centryczny nie jest całkowicie scentralizowany, nawet na poziomie lokalnym. Duże fragmenty brzegu zachowują znaczną autonomię. Ujęcie źródło-centryczne rozwinęło się dzięki postępowi technologii czujników, ale także lokalnych specjalizowanych sieci proksymalnych i bardzo tanich procesorów o znacznych zasobach obliczeniowych. W obu ujęciach bardzo różnorodnym lokalnym i coraz bardziej znormalizowanym globalnym trudno obecnie znaleźć bezpośredni wspólny mianownik. Poszukiwane są lekkie protokoły brzegowe dla sieci proksymalnych, nie o takim stopniu skomplikowania jak TCP/IP. Obecnie funkcjonuje wiele takich protokołów i nie ma wśród nich jednorodności. Walczą ze sobą różne standardy rozwijane i wspierane przez różne naukowo-przemysłowe grupy interesariuszy. A w tle czekają potencjalnie ogromne środki na rozwój zwycięskich standardów IoT (IIConsortium 2015). Na wyższym poziomie architektury IoT w każdej wersji wspólnym mianownikiem jest Internet, szczególnie w wersji IP v.6., a więc wspólne protokoły komunikacyjne, wspólne środowiska programistyczne i jednakowy dostęp.

Brzegowy, źródłowo i sygnałowo-centryczny IoT posiada zupełnie inne właściwości od głębszych czy wyższych struktur architektury IoT. Mówi się także że jest najtrudniejszym składnikiem globalnego IoT. Jest najbardziej zróżnicowany sprzętowo, obecnie najdroższy, i najbardziej zawodny z powodu działania w różnych warunkach środowiskowych. Zwiększającej się różnorodności konstrukcji czujników wykorzystujących do pomiaru różne zjawiska fizyczne i chemiczne, mechaniczne, optyczne, elektryczne, magnetyczne, kwantowe, biologiczne, nie da się znormalizować. Brzegowy IoT to nie tylko czujniki, to sterowniki, automatyka, urządzania wykonawcze, zawory, pompy, przełączniki, układy pomiarowo-kontrolne, elementy sprzężeń zwrotnych, itp. Brzegowy IoT to wiele rozwiązań własnościowych nie poddających się standaryzacji. Próbować normalizować można w pewnym zakresie interfejsy i stopnie wejściowe czujników i sterowników do systemu IoT poprzez znaczną różnorodność dzisiaj przewidywanych sieci proksymalnych. Standaryzacja przeniknie do brzegu IoT jeśli zaoferuje znacznie niższe koszty i wyższą niezawodność niż rozwiązań własnościowych. Akwizycja sygnałów, i konwersja do poziomu danych, dzisiaj robiona z milionów a w przyszłości z milionów bilionów czujników jest zagadnieniem przekraczającym dzisiejsze możliwości techniki (Smith 2016). Jednak uparcie podążamy w badaniach naukowych i przemysłowych w kierunku opanowania technik wytwarzania wielkiej różnorodności specjalizowanych sub-miniaturowych zwanych pyłkami, a przede wszystkim tanich czujników o bardzo niewielkim zapotrzebowaniu na energię, potrafiących samodzielnie zdobyć tą energię ze zmiennego chemicznie, termicznie czy elektromagnetycznie środowiska pracy, potrafiących samodzielnie skonfigurować się w sieć wymiany informacji z innymi czujnikami w pobliżu, potrafiących wybrać wśród siebie lidera odpowiedzialnego za przekazanie informacji wyżej, potrafiących zmienić lidera jeśli obecny pracuje nie tak jak potrzeba. Samo-konfigurowalne, autonomiczne energetycznie, relatywnie tanie, sieci czujnikowe są dzisiaj testowane w zastosowaniach w rolnictwie, monitoringu środowiska. Mikroczujniki są rozsiewane przypadkowo w obszarze ich potencjalnego działania. Na przyszłe potrzeby są to sieci niewielkie, ciągle stanowczo za małe. Skalowanie rozmiarów i funkcjonalności brzegowych sieci czujnikowych dla IoT jest przedmiotem badań. Brzegowa część IoT jest zupełnie inna dla różnych miejsc zbierania danych (Mach 2017). Nie tylko chodzi o zastosowane różne czujniki, ale także odmienną taktykę zbierania, zapisu i akwizycji sygnałów, dopasowaną do wymogów miejsca zastosowania. Węzłom sieci czujnikowej, poszczególnym jednostkom wykonawczym, i całej sieci przypisuje się, realizowane technicznie programistycznie i sprzętowo, atrybuty antropomorficzne takie jak: zapobiegliwość, agresywność, chciwość i zachłanność, zazdrość, przebiegłość, ale także zdolność przewidywania, podporządkowanie, leniwość, bierność. Takie cechy przypisywane węzłom, okazuje się, są konieczne do sprawnego wykonywania zadań nie tylko przez sieć czujnikową, ale także np. przez rój robotów wykonujących wspólne większe zadanie zrównoleglone na wiele jednostek funkcjonalnych. Zasoby pomiarowe czy wykonawcze w takich sieciach o zmiennych charakterystykach węzłów mogą być dynamicznie rekonfigurowane w celu efektywnego wykonania zadania. Zwiększenie napływu danych w pewnym miejscu na brzegu IoT wymaga rekonfiguracji sieci i skupienia zasobów w tym miejscu. Mówimy o dynamicznej relokacji zasobów. W innym przypadku krytyczne dane są tracone, za co odpowiada i za co karana jest sieć lokalna. Obciążenie roju większym zadaniem w pewnym miejscu brzegu IoT wymaga optymalnej rekonfiguracji zasobów, ale wykonywanej przez sam rój samodzielnie. Dla roju priorytetem jest wykonanie zadania, ale z pewnymi atrybutami jak: ekologiczność, minimalizacja energii, koszty, nie niszczenie mienia, czas i obszar działania, itp. Należy podkreślić, że decyzje rekonfiguracji zasobów brzegowych podejmowane są głównie lokalnie. To brzeg IoT decyduje o taktyce działania. To brzeg IoT zbiera dane i doświadczenia lokalne i decyduje co ewentualnie przesłać wyżej jako doświadczenie ogólniejsze przydatne szerzej. Sieć wyższa może oczywiście zapytać brzeg co słychać. Możliwość interrogacji jest konieczna. Widać w sieci IoT poziomy działań operacyjnych, taktycznych i strategicznych. Bez ciągłego dopływu danych z brzegu IoT jest głuchy i ślepy. Chyba że bazuje na poprzednich doświadczeniach i sztucznej inteligencji, ale to ciągle za mało.

Mówimy także o usługo-centrycznej, siecio-centrycznej, chmurocentrycznej, inaczej mówiąc telekomunikacyjnej definicji IoT. Specjaliści od telekomunikacji, przynajmniej niektórzy, twierdzą że poprzednio baza danych, Chmura oraz obecnie IoT jest w zasadzie częścią linii rozwojowej telekomunikacji, jako jej przyszłościowy pakiet usług (Slama 2000). Chmura abonencka, do indywidualnego użytku konsumenckiego, w wersji podstawowej bezpłatna, jest popularna i używana prawie przez wszystkich z nas, jak Adobe Creative Cloud, Microsoft OneDrive, Windows Live, SkyDrive, DropBox, Box, Dysk Google, i inne. Także Orange uruchomił usługi chmurowe, ale z jakichś względów wycofał się ostatnio z tego.Usługi sieciowe używane i cenione to coraz lepsza realizacja skomplikowanych zapytań, tłumacze wielojęzykowe, rozpoznawanie dźwięków, muzyki, obrazów, obiektów, miejsc, zaawansowana orientacja. Już jakiś czas temu można było zamówić, także u krajowych operatorów telekomunikacyjnych, takie usługi, jednak niestandaryzowane i tylko o charakterze własnościowym, jak nadzór nad osobami wymagającymi monitorowania kardiologicznego, ochrona nieruchomości, elementy inteligentnego domu, powiadamiania specjalistyczne, obliczenia w Chmurze, utrzymanie danych w bazie, itp. W ujęciu usługo-centrycznym istotą działania IoT są oferowane usługi wykorzystując znormalizowaną transmisję, wymianę, przechowywanie i przetwarzanie sygnałów i informacji, oraz efektywna współpraca z wielką rozmaitością funkcjonalnych sieci proksymalnych i dostępowych, wirtualizowanych a więc niezależna od operatora, tylko ukierunkowana na abonenta. To w znormalizowanych sieciach proksymalnych, dostępowych najniższego poziomu, do których podłączone są sprzętowo i programistycznie czujniki i efektory, realizowane są bezpośrednio podstawowe funkcjonalności Internetu Rzeczy. Sieci posiadają klasyczną architekturę obejmującą warstwy fizyczną, sieciową i aplikacyjną. Lokalne przetwarzanie danych, w terminalu abonenta, w lokalnej centrali dostawcy i oferowanie na takiej podstawie usług jest rozwiązaniem naturalnym, najtańszym, wyposażającym funkcjonalności przedmiotów w pewien stopień inteligencji i autonomiczność. W ujęciu telekomunikacyjnym IoT jest źródłem usług. Operator telekomunikacyjny jest zaangażowany w rozwój IoT na poziomie globalnym zapewniając działanie sieci szkieletowej oraz sieci dużych typu MAN, WAN, itp. Dostawcy usług IoT, tak jak dzisiaj znani nam dostawcy Internetu, czy energii elektrycznej, oferują użytkownikom indywidualnym, ale także firmom, przemysłowi i innym instytucjom, czyli abonentom, różny rodzaj usług, także platform do tworzenia usług. Dostatecznie duzi użytkownicy IoT, szczególnie przemysłowi będą zapewne budować własne zamknięte struktury IoT, w razie potrzeby łączone z usługami sieci globalnej. Jest to je-

den z bardzo realistycznych kierunków i scenariuszy rozwoju IoT. Nie operuje się tutaj bezpośrednio terminem superinteligencji sieciowej. Raczej mówimy o zwiększającej się różnorodności sieci proksymalnych i dostępowych, o wirtualizacji sieci i rozwoju na takim podłożu telekomunikacyjnym bardzo różnych usług.

Operuje się takimi terminami i skrótami jak oprogramowanie jako usługa SaaS, urządzenie jako usługa DaaS, platforma/ekosystem jako usługa PaaS, wspomagane zdrowie jako usługa HaaS, inteligencja obliczeniowa jako usługa IaaS, itp. Realizm tego kierunku rozwojowego IoT jest silnie wsparty potencjałem ekonomicznym i znacznym doświadczeniem dużych operatorów telekomunikacyjnych w takich obszarach jak współpraca pomiędzy nauką i przemysłem, oraz dynamiczny rozwój sieci i wprowadzaniem nowych technologii sprzętowych i programistycznych. IoT to sieć telekomunikacyjna w całej swojej dzisiejszej różnorodności, dalej komplikującej się przyszłości i usługi oferowane za jej pomocą. A czy usługi są inteligentne, zaawansowane czy proste, lokalne czy globalne to sprawa wtórna, a właściwie sprawa ceny, dostępności, popularności, zapotrzebowania, rozwoju, przewidywania tendencji rynkowych, itp. O rozwoju konkretnych usług decydować ma w skali globalnej państwo i duży przemysł, a w skali lokalnej indywidualny użytkownik. IoT staje się częścią istniejącego ale ciągle rozwijanego i ewoluującego systemu telekomunikacyjnego (Santana 2013), (Sarver 2017). W związku z czym obecny rozwój IoT jest w gestii umowy pomiędzy dostawcą i abonentem. Jednak gdzie to jest możliwe i dozwolone nie rezygnujemy w usługo-centrycznym IoT z szerszego usieciowienia rozwiązań lokalnych, szczególnie tych cieszących się powodzeniem rynku. Lokalna sieć dostępowa realizująca funkcje Internetu Przedmiotów może być wielopoziomowa realizując funkcjonalności dla mniejszych i dalej większych infrastruktur lokalnych. Już na tym najniższym poziomie, korzystając z danych sieci proksymalnej, realizowane jest zaawansowane przetwarzanie danych. Hierarchizacja sieci funkcjonalnych IIoT obejmuje warstwy własnościowe - proksymalną, dostępową, usługową i zewnętrzne. Transmisja wielkich ilości sygnałów odbywa się w znormalizowanych sieciach szkieletowych o praktycznie nieograniczonej przepustowości, a funkcjonalne wykorzystanie tych sygnałów, już jako konkretnych danych użytkowych, odbywa się w lokalnych sieciach proksymalnych i dostępowych o znacznej różnorodności. W zakresie IoT siecio-centrycznego jedna z pierwych na globalną skalę jest Nokia ze swoim właśnie uruchamianym środowiskiem biznesowym Nokia wordwide IoT network grid, ukierunkowanym na obsługę dostawców usług telekomunikacyjnych i przedsiębiorstw przede wszystkim z sektorów transportu, zdrowia, użyteczności publicznej i bezpieczeństwa. Nokia IoT grid ma zapewniać w skali globalnej połączenia IoT i umożliwiać ich zarządzanie. Utworzenie takiej usługi nie jest możliwe dzisiaj przez jedną firmę, nawet globalną. Konieczna jest współpraca wielu partnerów z różnych części świata. Konieczne jest przezwyciężenie wielu ograniczeń prawnych, zapewnienie bezpieczeństwa, możliwości sprawnego przełączania strumieni danych pomiędzy różnymi sieciami kablowymi, satelitarnymi i ruchomymi.

Definicja inteligencjo-centryczna odkreśla IoT jako rozproszoną inteligencję, prawie wyłącznie sztuczną inteligencję. Dane w takim ujęciu są konieczne, ale jedynie pomocnicze. Podobnie pomocnicza jest transmisja danych, która jest oczywista. To centralna i rozproszona inteligencja jest nieoczywista (Kellmereit 2013), (Chace 2015). Istotą IoT jest sztuczna inteligencja, maszynowa lub programistyczna, jej sposób postępowania dotyczący infrastruktury cywilizacyjnej, analityka, estymacja i predykcja zjawisk i zachowań, oraz stosunek do człowieka, a środkami do realizacji tych celów są zgromadzona wiedza, zasoby obliczeniowe, korzystanie z poprzednich i nowych danych, ciągłe uczenie się, oraz zbieranie nowych doświadczeń. Inteligencjo-centryczne ujęcie IoT też posiada warstwy lokalną i globalną, ale skala lokalna jest w pewnym sensie wtórna wobec globalnej, odwrotnie niż w ujęciu źródło-centrycznym. Warstwa lokalna, mówiąc w uproszczeniu, nadaje inteligencję rzeczom lokalnym, np. bliskim człowieka takim jak smartfon, kamera video, dron, inne gadżety. Jest to możliwe dzięki rozwojowi technologii. Najmniejsze urządzenia o podstawowej funkcjonalności analogicznej do PC mogą obecnie posiadać objętość 1 mm^3. Inteligentne rzeczy to jednak nadal termin wysoce nieprecyzyjny, a wręcz zupełnie nieprawdziwy, z inteligencją nie mający wiele wspólnego, a jednak powszechnie używany w języku popularnym, a także naukowym. Wojskowi używają terminu inteligentne pociski. W nauce nadużywa się terminu inteligentne czujniki. Autonomiczne samochody osobowe są inteligentne? W niektórych rozważaniach dotyczących inteligentnego IoT, prawdopodobnie w celu uniknięcia terminu inteligencja, rzeczom nadaje się inny, także mało precyzyjny atrybut ‘socjalne’. Rzeczy socjalne/społeczne to takie którym nadano w IoT dodatkowe wirtualne, przydatne, miękkie funkcjonalności i przez to stały się przyjazne, bardziej użyteczne, dopasowane, interfejsowane do nowej rzeczywistości IoT, a przez to właśnie uspołecznione, socjalizowane. Znowu pojawia się w inny sposób zagadnienie antropomorfizacji takiej rzeczy, na razie po prostu i tylko podłączonej kabelkiem lub łączem Wi-Fi do IoT. Marzeniem niektórych inteligencjo-centrystycznych grup projektantów i budowniczych IoT jest centralizacja, centralne gromadzenie wiedzy i budowa Wielkiego Brata (Chace 2015). Silnym argumentem za całkowicie scentralizowanym ujęciem IoT jest, że tej pełnej wiedzy w skali całej Ziemi nie jest wcale tak dużo, pod warunkiem że dysponuje się odpowiednimi zasobami inteligencji obliczeniowej, od których to zasobów nie jesteśmy daleko. Na razie jednak nie oznacza to, że warstwa lokalna jest mniej ważna. Dzisiaj, w skali globalnej budowy inteligentnego IoT są to wielkie ilości danych, wielkie zasoby obliczeniowe, duże zasoby zgromadzonej wiedzy, i inteligencja ukierunkowana na rozwiązywanie problemów globalnych. W skali lokalnej inteligentnego IoT są to ewentualnie dane ogólne i specjalistyczne charakterystyczne dla danej lokalizacji i inteligencja ukierunkowana na rozwiązywanie problemów lokalnych. Czyli budowa wielu Mniejszych Braci (DelMonte 2015).

Ogólną istotą sztucznej inteligencji dla IoT, i oczywiście nie tylko dla IoT, jest zawsze działanie w warunkach niepełnej informacji, nie zawsze wysokiej jakości danych, ograniczonego i zakłócanego pasma transmisji pomiędzy przedmiotami, maszynami, węzłami sieci, niepełnej polegalności i dostępności łączy transmisyjnych i sieci danych, zmieszanych danych z różnych źródeł – lokalnych i od innych maszyn, koniecznością przeprowadzenia obliczeń dla rozwiązań lokalnych poza warunkami centrum obliczeniowego, konieczność sięgania po dane odległe. Niewątpliwie, w takich warunkach pracy będzie działać wiele praktycznych, a więc nieidealnych systemów IoT. Nieidealność, skończona niezawodność, będzie stałym atrybutem takich coraz bardziej komplikujących się systemów. Stąd sztuczna inteligencja i umiejętność oceny błędnego działania jest niezbędna do ich funkcjonowania. W przypadku pełnych danych i prostych funkcjonalności inteligencja jest niekonieczna, wystarczy maszyna stanu. I wiele części IoT będzie działać korzystając z maszyn stanu i rozwiązań rutynowych, a nie będzie korzystać z bezpośredniej ingerencji sztucznej inteligencji. Na zewnątrz wygląda to jednak jak zachowanie inteligentne. Popadnięcie w rutynę przez pewne fragmenty algorytmicznego czy inteligentnego IoT także niesie pewne zagrożenie dla działania sieci globalnej. Nadmierne ufanie rutynie użytkownika IoT również posiada inne konsekwencje. Inteligencja IoT będzie musiała jednak w jakiejś formie czuwać cały czas w naszym interesie. W inteligencjo-centrycznym ujęciu IoT szczególne i znacznie rozszerzone znaczenie ma cyberbezpieczeństwo. Inteligentnemu IoT oddajemy znacznie więcej władzy niż IoT brzegowemu i usługowemu. Inteligencjo-centryczny IoT jest dodatkowo znacznie bardziej scentralizowany i takie centrum, centralny mózg systemu musi być specjalnie zabezpieczony. W kwestii zabezpieczenia mówimy o redundancji systemowej, funkcjonalnej, operacyjnej, technicznej, sprzętowej i programistycznej, a także geograficznej. Mówimy także o poważnym niebezpieczeństwie przyszłości spamowania IoT, nieuczciwości wirtualnej i sposobach zabezpieczenia przed nimi (Berglass 2015), (Brooks 2017). Konsekwencje decyzji centralnych w tym IoT mogą mieć znacznie większe skutki. Inteligencjo-centryczny IoT jest bardzo kuszącą wersją architektury, i wydaje się opcją najbardziej przyszłościową. Wersja ta jest intensywnie rozwijana w laboratoriach badawczych uczelnianych i korporacyjnych sztucznej inteligencji, ale pełnię swojego potencjału może pokazać dopiero po odpowiednim rozwinięciu brzegowego i usługowego IoT. Fragmenty inteligencjo-centrycznego IoT są testowane w warunkach pracy zbliżonych do rzeczywistych np. przez firmy GE, IBM, Cisco, i inne. Z punktu widzenia antropocentrycznego ciekawy będzie ten moment kiedy stosując nasze kryteria ilościowe i jakościowe uznamy, że sztuczna inteligencja osiągnęła właśnie poziom krytyczny. Poziom który określimy atrybutem autonomiczny, i który będzie wówczas musiał być sklasyfikowany prawnie.

Wiedzo-centryczna definicja IoT jest rodzajem podejścia hybrydowego. W pewien sposób jest powiązana z definicjami poprzednimi, technicznymi dano-, siecio-, i inteligencjo-centrycznymi, łącząc ich odmienne atrybuty, ale to nie wszystko. Wychodzi także istotnie poza technikę. Wiedzo-centryczny IoT musi mieć silną warstwę socjalną. Nie mówimy wszakże o społeczeństwie opartym na sztucznej inteligencji tylko o opartym na wiedzy. Różnica nie polega tylko na skali danych, jak lokalnej niewielkiej czy globalnej ogromnej, nie tylko na źródłach, sygnałach lokalnych, uważanych za składniki prostsze i nie

tak kluczowe jak wiedza. Wiedza jest pozyskiwana z różnych źródeł, historycznych, nowych, z wielkiej ilości znormalizowanych danych. Uważa się, że IoT będzie w przyszłości służył w znacznej mierze do generacji nowej wiedzy. IoT jako generator wiedzy ma być motorem innowacji i postępu. Celem nadrzędnym IoT ewoluującego w Internet Wiedzy IoK jest w pewnym sensie jej automatyczna produkcja. Do tej pory produkcja wiedzy była nieodłącznym atrybutem człowieka. To ma się zmienić, i jeśli tak się stanie, przeobrazić cywilizację. A przy okazji mamy oczywiście odnieść z produkcji wiedzy szereg korzyści, opisanych poprzednio. Z produkcją wiedzy, Internetem Wiedzy i Społeczeństwem Wiedzy wiąże się wiele korzyści ale i zagrożeń. Niektóre widzimy już dziś. Mówimy o kryzysie gospodarczym w Europie i konieczności reindustrializacji. Ta pilna, niemal ratunkowa potrzeba reindustrializacji jest wielką szansą dla Europy, dla Polski na odbudowanie nowej generacji przemysłu wytwórczego z wbudowanym w niego systemem nerwowym i krwionośnym, silnym szkieletem IoT (Smith 2016). Europa produkuje wiedzę a poza Europą wykorzystując intensywnie i prawie za darmo tą wiedzę budowany jest przemysł wytwórczy. Europa wprowadza IoT do gospodarki i biznesu jako jeden z liderów technologii ICT. Jeśli nie wyważone będą wszystkie czynniki to sama nie chroniona wiedza, i jej produkcja, przecież nie bez kosztowa, jest śmiertelną pułapką. A ochrona wiedzy dzisiaj, w czasach kiedy uczeni apelują o powszechność standardu ‘open source’, jest bardzo trudna, o ile w ogóle możliwa. Internet Wiedzy IoK jest przyszłością, ale z wieloma zastrzeżeniami. Z niektórych z nich nie zdajemy sobie dzisiaj sprawy. Były wojny o zasoby, terytoria, ale o wiedzę? Potężny IoK może stać się podłożem nowych pozytywnych kierunków rozwoju społeczeństwa, ale także dyskryminacji, wyzysku, wykluczenia, i cyfrowego podziału świata o trudnych do wyobrażenia konsekwencjach. Można pokazać, używając już dzisiaj realistycznych argumentów technicznych, że przyszły IoK może mieć siłę rażenia broni jądrowej. IoK może być bronią masowego rażenia. Terminy Społeczeństwo Wiedzy, także IoK, IoE, IoT są czasami intencjonalnie nadużywane w celach politycznych, używane bezrefleksyjnie przez wielu komentatorów, epatuje się tymi terminami w nieadekwatnych sytuacjach, a dzisiejsza gospodarka to boleśnie weryfikuje. U nas w Polsce potrzebne są pilnie centralne, systemowe inwestycje w budowę infrastruktury IoT, skupione wokół wyraźnych priorytetów gospodarczych, które będą budowały łącznie z inwestycjami biznesowymi platformę reindustrializacji kraju, stymulowały odbudowę przemysłu wytwórczego, tworzenie nowego środowiska dla gospodarowania, odnawiały tradycyjne i tworzyły nowe usługi przyjazne człowiekowi.

Bez wątpienia związana z wiedzo-centryczną, przedmioto-centryczna, ontologiczna i aksjologiczna definicja IoT wydaje się już daleko odchodzić od nauk technicznych, ale warto ją tutaj przywołać choćby w dużym skrócie bo jest chyba najbardziej naturalna, najbliższa humanistycznemu myśleniu człowieka. Przy okazji ujawnione mogą być subtelne formalne różnice pomiędzy używanymi określeniami Internet Przedmiotów czy Rzeczy, całkowicie pomijane w języku potocznym, a w rzeczywistości pogłębiające problem analizy tego nowego bardzo złożonego zjawiska. Przedmiot, obiekt, coś, rzecz obserwowana, jest jednym z podstawowych pojęć ontologii, używanym w kontraście do podmiotu czyli obserwatora. Rzecz, samodzielny byt jednostkowy jest kategorią przedmiotów fizycznych o określonych charakterystykach. Czyli Internet Przedmiotów, nadający obiektom inteligencję, autonomię i samo-świadomość, choćby ograniczoną i lokalną, potencjalnie zmienia ontologię. W przyszłości albo wprowadza nową kategorię ontologiczną, albo zaciera różnice pomiędzy obserwatorem i obserwowanym. Internet Rzeczy zmienia potencjalnie bardzo poważnie kategorię przedmiotów fizycznych i zakres ich zupełnych charakterystyk. Przedmioto-centryczny IoT jest kategorią albo zmieniającą ontologię poprzez pewnego rodzaju upodmiotowienie rzeczy, zapewne nie dzisiaj i jutro ale być może w przyszłości, albo nadającą tylko nowe znaczenie rzeczom. Musimy się zdecydować jak to traktować, albo rozwój techniki za nas zdecyduje. To ostatnie jest bardziej prawdopodobne. Pada wówczas dalsze naturalne pytanie o wartość o aksjologię takiego nowego skomplikowanego bytu jak IoK, zawieszanego między przedmiotem i podmiotem, obserwatorem i obserwowanym, posiadającego w jakimś stopniu coś co przypomina świadomość, emocjonalność, osąd i swoją moralność? Nie kontynuujemy tutaj tego być może bardzo rozwojowego tematu, dotyczącego także ewolucji samego człowieka w środowisku Internetu Wiedzy. Trudno sobie wyobrazić abyśmy nie byli podatni na zmiany pod taką presją. Trzeba jednak dodać, że praktyka tworzonego dzisiaj IoT musi koniecznie utworzyć już teraz, jak najszybciej, rodzaj własnościowego abstraktu, bytu nazywanego ‘Rzeczą’ i obejmującego rzeczy, aplikacje i usługi. Inaczej nie będziemy wiedzieli co dokładnie oznacza Internet Rzeczy. Właściwości takiej rzeczy mogą być rzeczywiste lub wirtualne. Taka rzecz posiada funkcje lub jest metodą i może wymieniać informacje w sposób horyzontalny, wertykalny lub mieszany. Poziomy abstrakcji dla takich rzeczy zaczynają się od encji fizycznej i podążają poprzez uniwersalny opis rzeczy, warstwę aplikacji i usług, do architektury i modelu odniesienia.

Próbując nieco arbitralnie sumować te podejścia mamy IoT jako dostarczyciela mniej lub bardziej zaawansowanych czy trywialnych usług dla infrastruktury, gospodarki i użytkowników indywidualnych, bardzo liczne źródła danych i ich analitykę, bazy danych z odkrywaniem wiedzy, fabrykę wiedzy, rozproszoną inteligencję, aktywną usługę telekomunikacyjną, mobilne środowisko socjalne, ale też międzymaszynowe. Czy te charakterystyki rzeczywiście sumują się dzisiaj, i na razie tylko dzisiaj, nad jakimś użytecznym wspólnym mianownikiem? Zapewne jest nim zwiększona, lecz akceptowana funkcjonalność rzeczy, w tym ich wzrastająca autonomia działania. Ale to daleko nie wszystko. IoT oparty na wiedzy, antropomorfizowany, ma szansę stać się bardzo szybko, prawie jutro, budowniczym nowego rodzaju aktywnej infrastruktury cywilizacyjnej, obejmującej warstwy gospodarcze i społeczne, wspomagającej rozwój społeczny i kulturalny. Czy naprawdę jeszcze tego już dzisiaj nie obserwujemy? Droga do wyższych poziomów jest jeszcze dość daleka. Jednak chyba nie widać na niej dzisiaj z naukowego punktu widzenia jakiejś absolutnej przeszkody nie do pokonania, szczególnie przy zrównoważonym technicznym, gospodarczym i społecznym rozwoju ewolucyjnym. Jednocześnie nie widać jeszcze ani jakiegoś wielkiego, zasadniczego przełomu technologicznego ani socjologicznego uzasadniającego taką skalę czekających nas potencjalnie przemian społecznych. Takim przełomem będzie inteligencja emocjonalna maszyny i jej elementy w postaci samoświadomości i moralności. Jakiej moralności, ludzkiej czy maszynowej, kontrolowanej, zarządzanej czy autonomicznej? Nie tylko to. Przełomem będzie produkcja dowolnych ilości energii tanim kosztem (iter.org). Przełomem będzie produkcja żywności poza klasycznym rolnictwem metodami syntezy fotonicznej i biochemicznej białek. Przełomem będzie opracowanie przez inżynierię genetyczną praktycznych, szybkich i tanich metod syntezy dowolnego DNA i opanowanie wielu chorób ludzi, zwierząt i roślin. I wiele innych. I co najważniejsze, przełomem będzie zdobywanie znacznej ilości wiedzy, także tanim kosztem. W wielu z tych dziedzin odniesiono bardzo obiecujące początkowe sukcesy, pozwalające na stawianie odważniejszych prognoz rozwojowych. Wymieńmy jeszcze raz, uporczywie powtarzając, te dziedziny gdzie wiedzo-centryczny IoT, czyli IoK, jest rozwijany przez naukę i przemysł jako potencjalna platforma rozwojowa społeczeństwa opartego na wiedzy (Connoly 2016). IoK spełni pokładane w nim nadzieje jeśli zostanie oswojony i zaakceptowany przez przyszłe społeczeństwo, co nie jest dzisiaj oczywiste, jeśli nie pójdzie w kierunku wspomnianego „gadżeciarstwa”, jeśli opanuje wymienione znaczne niebezpieczeństwa oraz uniknie pułapek rozwojowych, jeśli skoncentruje się na fundamentalnych potrzebach decydujących o rozwoju społeczeństwa czyli zapewnieniu energii i żywności, zdrowiu, bezpieczeństwie, transporcie, warunkach życia, edukacji i nauki, gospodarowaniu, infrastrukturze cywilizacyjnej oraz dobrostanie człowieka, obejmującym kulturę, odpoczynek, sport, rozrywkę, itp. Wreszcie, jeśli nie zagrozi bytowi człowieka (DelMonte 2016).

Przewidując taki rozwój IoT/IoK, i ukryte za tym rozwojem wielkie finanse rzędu trylionów dolarów na następne dziesięciolecie i biliony podłączonych urządzeń, a więc nie bez przyczyny firma Cisco, jeden z największych światowych producentów oprogramowania i sprzętu IoT, nazwała go już jakiś czas temu Internetem Wszystkiego IoE [ioeassessment.cisco.com]. Terminy IoT, IoK, IoE są czasami używane wymiennie, choć nie oznaczają dokładnie tego samego. Termin IoE oznacza ogromną przewagę transportu danych M2M w przyszłości nad innymi rodzajami funkcjonalności. Czasami termin IoT uzupełnia się o usługi, z czego powstaje jeszcze inny używany skrót IoT&S. My skupiamy się na przejściu IoT pomiędzy RIoT i IIoT. Do realizacji takiego sprawnego przejścia konieczne jest istnienie oprócz laboratoriów badawczych także pełnego ekosystemu IoT zawierającego wszystkie komponenty umożliwiające prowadzenie działalności gospodarczej, otoczenia prawnego działalności, dostawców, konsumentów, klientów, abonentów usług, i podłączenie tych komponentów do ich lokalnych i zdalnych urządzeń IoT, interfejsów i paneli użytkownika, sieci, bramek sprzętowych, narzędzi analityki biznesowej, magazynów danych, oraz adekwatnych narzędzi bezpieczeństwa. Dostępna publicznie, wielośródłowa analityka biznesowa pokazuje, że IoT zmienia najbardziej biznes – obniża koszty operacyjne, zwiększa możliwości

produkcyjne, rozszerza rynki i rozwija nowe produkty. Mówi się, że mądre organizacje biznesowe stosują analitykę, a odnoszące sukcesy wbudowują ją w strategię działania. Adaptacja rozwiązań IoT będzie w najbliższym czasie zdecydowanie największa w gospodarce. Pod względem masywności zastosowań na drugim miejscu jest rząd i administracja centralna i lokalna. Odbiorca końcowy, indywidualny konsument będzie najwolniej transformowany przez IoT. Taka kolejność transformacji może być zaskoczeniem dla niespecjalisty. Przemysł wytwórczy i usługi aby przeżyć do jutra muszą rozpocząć natychmiast digitalizację (Rayes 2016), (Vermesan 2016). Digitalizacja obejmuje tam także zarządzanie łańcuchem dostaw elementów do produkcji czy dostaw rynkowych. Wiele sektorów podlega digitalizacji od jakiegoś czasu. Obszary podlegające transformacji powiększają się. Obszary nie transformowane mogą być za jakiś czas marginalizowane. Administracja i samorządy muszą digitalizować się z wielu innych względów niż przemysł. Trudno wyobrazić sobie sprawną administrację bez informacji. Klient indywidualny w zasadzie nic nie musi. Jeśli chce mieć więcej usług własnych, prywatnych jedynie dla siebie to je kupi, ale jeśli będą opłacalne. Wiele usług dostanie i tak z nowoczesnym smartfonem, z kupowanym nowym sprzętem AGD, samochodem, w nowoczesnej infrastrukturze mieszkaniowej, osiedlowej i miejskiej. W cenę takiego inteligentnego sprzętu będzie wliczony abonament inteligentnej usługi sieciowej (Miller 2015). Usługi infrastrukturalne IoT dostanie za podatki. Nikt nie będzie pytał indywidualnego konsumenta czy chce czy nie chce się usieciowić i transformować w kierunku IoT. Handel, przemysł i usługi, oraz administracja zrobią to w dużej mierze za niego, szybko i niezauważalnie. Stawka jest zbyt duża aby ten obszar rynku zostawić w spokoju. Stawka jest kolosalna, dotyczy powstawania na naszych oczach masywnego kierunku rozwoju społecznego. Tak duża stawka jest i musi być zagospodarowywana przez różnego rodzaju organizacje społeczne i gospodarcze, jak Instytut IEEE (iot.ieee.org), Fundacja Prpl (Prpl 2016), IIConsortium, i inne .

Organizacje IoT

Krótka odpowiedź na pytanie co zadecyduje o powszechności IoT jest w zasadzie prosta. Wymienić można zaledwie kilka najważniejszych czynników technicznych i pozatechnicznych, jak powszechna standaryzacja, niskie koszty, szeroka akceptacja społeczna, prostota, nieuciążliwość, bezpieczeństwo, realizacja potrzebnych funkcjonalności metodami znacznie prostszymi niż dotychczas, generacja nowych funkcjonalności na które jest duże zapotrzebowanie, itp. Internet przemysłowy, gospodarczy, profesjonalny, a w tym IoT i IIoT, podlega właśnie szybkim procesom standaryzacji. Jest to jednak kierunek rozwoju trudniejszy i wolniejszy niż w przypadku otwartego Internetu. Procesy standaryzacyjne podążają znaną ścieżką w ścisłej współpracy nauki i przemysłu, podobnie do standaryzacji innych wcześniej rozwijanych obszarów cywilizacji technicznej, takich jak np. ICT. Konieczne jest tutaj przezwyciężanie konfliktów interesów pomiędzy różnymi grupami dużych interesariuszy. Robi się to poprzez tworzenie międzynarodowych kolaboracji, stowarzyszeń, konsorcjów i grup roboczych o charakterze naukowo-technicznym, politycznym, gospodarczym, lobbystycznym, także społecznym. Są to jednak najczęściej dobrze umocowane i silne grupy społecznościowe, na ogół otwarte, które w mniejszym lub większym stopniu podlegają formalizacji. Są to także jeszcze bardziej formalne grupy naukowo – przemysłowo – finansowe, raczej zamknięte, półotwarte, działające pod protektoratem dużych i wpływowych organizacji lobbystycznych o globalnym zasięgu. Tych najważniejszych grup IoT obu rodzajów o zasięgu globalnym jest kilka. Jednocześnie i konkurują one ze sobą i współpracują. Znacznie wcześniej utworzone, bardzo liczne, podobne ciała dla Internetu obejmują także organizacje standaryzacyjne, gospodarcze, pro-innowacyjne, społecznościowe, finansowo-biznesowe, lobbystyczne, itp. Dzisiaj działają także na rzecz IoT. Wymieńmy tutaj jedynie przykładowo kilka z nich, o różnym obszarze działania w nauce, przemyśle i biznesie, i o szerokim zasięgu międzynarodowym. Stowarzyszenie Internetowe IA – Internet Association (internetassociation.org) jest silną, wpływową, przemysłową i ekonomiczną, także polityczną organizacją lobbystyczną, pro-zatrudnieniową, z siedzibą w Washington DC, działającą na terenie USA głownie w obszarze zapewnienia pełnej wolności, innowacji i wzrostu ekonomicznego sieci Internet. IA jako reprezentant najbardziej znanych firm technologicznych wyraża opinie w sprawach politycznych i gospodarczych podczas prac senatu USA i działań biura Prezydenta. Głośnym echem w USA i świecie odbił się otwarty list IA z początku roku 2017, do nowo wybranego Prezydenta, w sprawie uregulowań ekonomicznych i gospodarczych Internetu, w tym IoT, i jego kierunków rozwoju. Towarzystwo Internetowe ISOC – Internet Society (internetsociety.org) jest niezależnym międzynarodowym ciałem opiniotwórczym w zakresie utrzymania, budowy i polityki Internetu, standardów technicznych i przyszłego rozwoju. Z międzynarodowym Towarzystwem Internetowym związane są internetowe towarzystwa krajowe, jako oddziały ISOC posiadające lokalnie status stowarzyszeń. Na takiej zasadzie działa Polskie Towarzystwo Internetowe ISOC Poland. ISOC działa głównie w warstwie społecznej i naukowo-technicznej ale także w razie potrzeby w politycznej. Stowarzyszenie Badaczy Internetu AoIR – Association of Internet Researchers (aoir.org) jest otwartą, członkowską organizacją akademicką i naukową poszukującą dalszego, interdyscyplinarnego, etycznego rozwoju tego obszaru także poza dziedzinami tradycyjnymi, eksploatowanymi obecnie. Działa poprzez publikacje naukowe opracowywane przez grupy robocze i organizowanie corocznych konferencji. Konferencja AoIR 2017 jest organizowana pod koniec roku w Estonii, jako jednym z najbardziej cyfrowo zaawansowanych krajów świata. Stowarzyszenie Marketingu Internetowego IMA – Internet marketing Association network (imanetwork.org) jest członkowską organizacją zawodową budującą jedną z największych baz danych instytucji związanych ze sprzedażą, marketingiem, biznesem właścicielskim, programowaniem i twórczym rozwojem Internetu biznesowego, także w kierunku biznesowego IoT. Organizuje okresowe konferencje IMPACT o zasięgu globalnym dotyczące kierunków rozwoju biznesu i marketingu internetowego. Podobną organizacją jest eMA – e-Marketing Association (emarketingassociation.com). Internetowe Stowarzyszenie Handlowe ICA – Internet Commerce Association jest organizacją niedochodową, orędownikiem praw i interesów właścicieli domen i dostawców usług Internetu i IoT. Niektóre z tych organizacji internetowych wprowadzają własne metryki dotyczące oceny ilościowej i jakościowej internetowej działalności gospodarczej, handlowej a także społecznościowej.

Konsorcjum Internetu Przemysłowego IIC – Industrial Internet Consortium (iiconsortium.org) jest organizacją członkowską grupującą zainteresowane instytucje standaryzacją techniczną i logistyczną w zakresie najlepszych praktyk i procesów przemysłowych wykorzystujących Internet. IIC powołuje swoje zespoły robocze opracowujące dokumenty odniesienia w tym obszarze. Podejmuje różne inicjatywy globalne jak Koalicję Interoperacyjności Internetu Przemysłowego I^3C dotyczącą takich obszarów jak: cyfryzacja i usieciowienie przemysłu, energetyka, opieka zdrowotna, produkcja przemysłowa, inteligentne miasta, transport. Organizuje okresowy kongres IIoT o charakterze międzynarodowym i dotyczący rozwoju i wdrażania praktycznych aplikacji IIoT (iotworldcongress.com). Publikuje artykuły techniczne, noty aplikacyjne, analizy przypadków, raporty dotyczące rozwoju innowacji dzięki Internetowi Przemysłowemu, rozwija swój kluczowy produkt – Architekturę Odniesienia Przemysłowego Internetu Przedmiotów IIRA – obecnie dostępną w wersjach 1.7 i 1.8. IIRA jest obszernym dokumentem opracowanym przez wieloautorskie zespoły robocze IIC, zredagowanym przez przedstawicieli między innymi takich firm jak IBM, GE, Fujitsu, Oracle, Intel, Cisco, HP, omawiającym aspekty biznesowe, użytkowe, funkcjonalne, implementacyjne, bezpieczeństwa, zarządzania danymi i systemami, integracyjności i interoperacyjności, oraz inteligentnych systemów sterowania i automatyki przemysłowej. IIC z udziałem swoich członków oferuje środowiska rozwojowo-testowe, dla aplikacji Przemysłowego Internetu Przedmiotów, zlokalizowane w rzeczywistych warunkach produkcyjnych, udostępnionych do celów badawczych przez członków konsorcjum. Każde środowisko jest opracowywane przez grupę członków IIC z nauki i z przemysłu specjalizujących się w danym sektorze przemysłu, ochrony zdrowia, środowiska naturalnego, bezpieczeństwa, itp. Dostępne dla członków środowiska testowe dotyczą na przykład: inteligentnych municypalnych systemów wodociągowych, mikrosieci energetycznych, monitoringu procesów przemysłowych, rolnictwa precyzyjnego, inteligentnych fabryk, transportu lotniczego, lokalnych systemów opieki zdrowotnej, i wielu innych. Jednym z badanych zagadnień w środowiskach testowych jest inteligencja brzegowa IIoT. Jest ona lokalizowana na wejściu systemu, tam gdzie znajdują się czujniki, aktuatory, sterowniki pojedynczych urządzeń, interfejsy aplikacyjne API, oraz interfejs od podstawowej domeny sterowania aparaturą przemysłową do domen wyższych, informacyjnej i operacyjnej. Poziom brzegowy IIoT, zawierający domenę sterowania, jest obsługiwany przez sieci proksymalną i dostępową. Dalej, według wytycznych dokumentu IIRA, korzystający z danych poziomu brzegowego, poziom platformy produkcyjnej IoT łączy się z poziomem przedsiębiorstwa i jest obsługiwany przez sieć

usługową. Poziom przedsiębiorstwa zawiera domeny aplikacyjne i biznesowe, dalej połączone w miarę potrzeby z zewnętrznym Internetem.

Platforma Industrie 4.0 (i4.0) jest łączoną rządową i naukowo–przemysłową organizacją niemiecką zarządzaną przez reprezentantów ministerstw gospodarki i energii, edukacji i badań naukowych, wysokich przedstawicieli przemysłu, nauki oraz związków zawodowych. Platforma działa poprzez tematyczne grupy robocze, koordynowane przez komitet sterujący. Grupy robocze opracowują dokumenty dotyczące różnych aspektów digitalizacji przemysłu, a w tym: architektury odniesienia, standardy i normy; badania i innowacje; bezpieczeństwo systemów sieciowych; ramy prawne; oraz praca, edukacja i szkolenie. Poprzez swoją znaczną aktywność, i trafność wyboru kierunków działania, mimo konkretnego ukierunkowania na rozwój i cyfryzację gospodarki niemieckiej, Platforma Industrie 4.0 stała się wzorem dla analogicznych organizacji w Europie. Opracowania i4.0 dotyczące przemysłowego IoT są traktowane praktycznie na całym świecie jako dokumenty odniesienia. We Francji taką organizacją, współpracującą z i4.0 we wszystkich wymienionych obszarach, jest Alliance Industrie du Futur l'AIF. Platforma i4.0 współpracuje także z amerykańskim Konsorcjum Internetu Przemysłowego IIC i Japońską organizacją Robot Revolution Initiative. Opracowywane są scenariusze rozwoju przemysłu wytwórczego ukierunkowane na potrzeby klientów. Ogólne scenariusze, pisane w formule top-down, posiadają formę archetypów rozwoju przemysłu umożliwionego przez nowe technologie produkcyjne i cyfrowe. Scenariusze są uzupełnione przez liczne gromadzone przypadki użycia IoT, niektóre formalnie opisane w języku UML, wdrożenia pilotowe, stanowiska testowe i prototypy badawcze. Całość dokumentacji posiada charakter aktywnego, politycznego, gospodarczego i logistycznego zachęcenia przedsiębiorstw do zaangażowania się w przemianę cyfrową przemysłu. Platforma i40 promuje rozwój technologii IoT, wymianę informacji o takich technologiach i jej wdrożeniach, oraz powstawanie otwartej infrastruktury testowej dostępnej dla jak największej liczby małych i średnich przedsiębiorstw, na zasadzie współpracy i zaufania a nie konkurencji. Wnioski z działania otwartych laboratoriów budowy infrastruktury testowej są wykorzystywane do opracowywania standardów przez adekwatne grupy robocze i4.0. Głównym dokumentem standaryzacyjnym i4.0, którego myślą przewodnią jest opracowanie jednolitej strategii stworzenia wspólnego przemysłowego europejskiego rynku cyfrowego, jest Reference Architecture Model Industrie 4.0 – RAMI 4.0. Pierwsza wersja dokumentu została opublikowana pod koniec 2016 roku i dotyczy sektora przemysłowego wewnątrz Internetu Przedmiotów i Usług – IoTS. Kolejna wersja będzie obejmować również robotykę i technologie produkcji addytywnej. Industrie 4.0 promuje edukację kadry zawodowej w zakresie nowych technologii, poprzez współpracę uniwersytetów, szkół zawodowych, instytucji naukowych i przemysłu innowacyjnego. Celem edukacji jest nadążenie ze zmianami kompetencji i organizacji pracy za potrzebami nowego przemysłowego rynku cyfrowego. Platforma i4.0 łączy i doprowadza finalnie do scalenia systemów produkcyjnych z technologiami informacyjnymi i komunikacyjnymi. Łączy dane klientów z danymi maszyn produkcyjnych. Rozwija technologie komunikacji M2M. Składniki takiego systemu i maszyny autonomicznie zarządzają produkcją w sposób elastyczny, sprawny i oszczędzający zasoby. Platforma i4.0 określa zalety wprowadzenia jednolitego cyfrowego rynku przemysłowego jako: wyższa jakość, sprawność i elastyczność produkcji, zwiększenie roli standaryzacji, szybsza droga produktu na rynek, ustawiczny benchmarking i poprawianie produktów, poprawienie warunków konkurencyjności pomiędzy silnymi partnerami biznesowymi, większe możliwości rynku pracy, tworzenie atrakcyjnych interdyscyplinarnych miejsc pracy na granicy wielu innowacyjnych technologii oraz ICT, powstanie nowych usług i modeli biznesowych. Opracowania i4.0, wskutek wspomagania rządowego, mają charakter precyzyjnego i systemowego rozwiązania całej problematyki transformacji przemysłu, gospodarki i ich otoczenia społecznego pomiędzy etapami analogowym i w pełni cyfrowym.

Konsorcjum OFC – OpenFog (openfogconsortium.org) jest publiczno-prywatnym, naukowo-przemysłowym ekosystemem utworzonym w celu przyspieszenia i adaptacji technologii obliczeń mgłowych w celu rozwiązania wielu problemów technicznych takich jak ograniczenie pasma, latencja aplikacji czasowo krytycznych, zagadnień transmisji danych i komunikacji, sztucznej inteligencji, robotyki w IoT, w Internecie Dotykowym, oraz w innych zaawansowanych koncepcjach cyfryzacji świata. Konsorcjum OpenFog zostało utworzone w 2015 r. przez największe światowe firmy ICT jak ARM, Cisco, Dell, Microsoft i Princeton University. OpenFog w pewnym sensie nawiązuje do działania Konsorcjum Open Cloud, obecnie Open Commons, a także Cloud Standards Customer Council CSCC, ponieważ technologia Fog jest z założenia architektonicznym rozszerzeniem technologii Cloud. W pewnych obszarach obie architektury się pokrywają i uzupełniają. W zakresie chmury dla IoT jednym z najważniejszych dokumentów odniesienia jest CSCC Cloud Customer Architecture for IoT, powstały w roku 2016. Dokument ten odnosi się także do wymienionego poprzednio dokumentu Konsorcjum Internetu Przemysłowego IIRA, co jest dowodem na pewną, nawet nie usankcjonowaną formalnie, konwergencję wysiłków i opracowań dotyczących IoT, powstałych w nieco różnych, ale zawsze dość szerokich środowiskach społecznych, naukowych, biznesowych, przemysłowych i administracyjnych. Opracowania OpenFog podkreślają heterogeniczność obecnego etapu rozwoju IoT i przedstawiają raczej punkt widzenia różnorodnego klienta systemu niż jego producenta. Wymieniane są różnice obecnych wymagań na funkcjonalne systemy IoT dla różnych sektorów biznesu i gospodarki. Pogłębiona analiza takich różnic i ich cech formalnych prowadzi do określenia ogólnych i wspólnych charakterystyk architektury IoT. Z lektury takich dokumentów architektonicznych dla IoT, opracowanych ostatnio różnymi metodami przez IIC, i4.0, SMAC, międzynarodowe społecznościowe zespoły robocze, formalne zespoły standaryzacyjne IEEE, analityczne firmy komercyjne, wyłania się obecnie obraz nowego, złożonego bytu obdarzonego wieloma wspólnymi atrybutami. Początkowo założenie na IoT było inne, znacznie prostsze polegające na dołożeniu relatywnie nieskomplikowanych dodatkowych funkcjonalności do sieci web. A to tak się w międzyczasie skomplikowało dokładając do złożonej warstwy technicznej warstwę społeczną. Konsorcjum OpenFog analizuje atrybuty IoT i sugeruje architektury ich realizacji w ekosystemie. Skalowalność jest wymaganą cechą systemów IoT umożliwiającą dodawanie wielu czujników i aktuatorów połączonych w sieć, przyjmowanie większej ilości informacji, oraz zwiększanie możliwości obliczeniowych w celu przetworzenia tej informacji. Zaawansowane systemy IoT są zależne od analizy wielkich ilości danych korzystając z technologii określanych w skrócie Big Data. Z wielkich zbiorów danych ekstrakcji podlegają poszukiwane wzory dokładające się do budowy decyzji i przyszłych działań. Wyszukiwanie wzorów danych ze strumieni video wymaga zastosowania znacznych mocy obliczeniowych. Wydobywanie danych z wielu dużych zbiorów heterogenicznych będzie cechą charakterystyczną systemów IoT. Systemy IoT korzystają z platform obliczeniowych w chmurze. Technologia Cloud Computing oferuje znaczne adaptowalne do wymogów metody archiwizowania danych i ich przetwarzania. Systemy IoT często pracują w czasie rzeczywistym. Niektóre rodzaje analizowanych danych strumieniowych wymagają reakcji na pojawiające się zdarzenia. Nowe zdarzenia są porównywane z historycznymi oraz z danymi statycznymi. Wychwytywane są zdarzenia anomalne, prowadzące potencjalnie do niebezpieczeństwa. Oceniane są przyczyny wystąpienia takich zdarzeń, albo jako awarie sprzętowe czy programistyczne, albo działanie intencjonalne. Rozproszenie przestrzenne jest cechą większości systemów IoT. Skala obejmuje budynki, firmowe obszary własnościowe, miasta, i zasięg globalny. Rozproszenie obejmuje wszystkie warstwy architektoniczne IoT, interfejsy i źródła mobilne, akwizycję, magazyny i przetwarzanie danych. Przetwarzanie zachodzi centralnie w chmurze, ale także w miarę potrzeby na brzegu sieci. IoT posiada strukturę heterogeniczną w sensie czujników, sterowników, rodzajów sieci działających pomiędzy czujnikami i metod przetwarzania informacji. Podłączenie takiej rozmaitości urządzań i rodzajów oprogramowania do Internetu wymaga zastosowania bramki IoT. Sieć IoT musi zapewniać prywatność i bezpieczeństwo, a przez to budzić zaufanie użytkownika. Zapewnienie tych cech w sieci rozproszonej i heterogenicznej jest bardzo trudnym problemem technicznym. Konieczne jest zapewnienie bezpieczeństwa danych. Na ogół zagadnienia bezpieczeństwa są rozwiązywane i skalowane wraz z rozwojem konkretnego systemu IoT. Systemy IoT muszą być zgodne ze sobą na pewnym poziomie architektury. Powinny spełniać normy ogólne przemysłowe i prawne, a także realizować funkcjonalności właścicielskie. Systemy IoT muszą wypełniać warunki integralności wewnętrznej i zewnętrznej. Stosowane w warunkach przemysłowych muszą być elementem współdziałającym konstruktywnie ze środowiskiem pracy. Wymienione powyżej atrybuty IoT są uwzględniane w dokumecie odniesienia OpenFog.

Nieformalne konsorcjum przemysłowo-gospodarcze SMAC jest skupione wokół rozwijanej już od 2010 roku koncepcji 'holistycznego' czteroskładnikowego standardu programistycznego Social, Mobile, Analytics and Cloud computing dla nowej generacji biznesu cyfrowego. SMAC jest znacznym rozszerzeniem wcześniej tworzo-

nej grupy środowisk programistycznych dotyczących planowania zasobów przedsiębiorstwa, typu ERC. Ideologia SMAC bazuje na archetypie konwersji heterogenicznych danych w informacje, i następnie wykorzystaniu czy transformacji informacji w wiedzę, i dalej w bazujące na wiedzy decyzje i potencjalnie w sukces biznesowy. Informacja jest tutaj rozumiana jako zbiór danych tworzących przydatny sens kontekstowy. Można wymienić szereg firm z sektorów ICT, bezpieczeństwa, inteligencji biznesowej, itp, rozwijające i stosujące platformę programistyczną SMAC jak SAP, IBM, HP, Oracle, ACSG, Cognizant, Genpact, Medtronic, Cinqueon, Infosys, i wiele innych. SMAC usytuowany pomiędzy i coraz bardziej skorelowany z IoT, Biga Data, Apache Hadoop, sztuczną inteligencją, sieciami społecznymi, jest ciągle rozwijanych i dość szeroko stosownym w praktyce projektem budowy ekosystemu analityczno-programistycznego dla nowego uniwersalnego modelu przedsiębiorstwa cyfrowego, realizacji biznesowych operacji cyfrowych, oraz aplikacji adekwatnych technologii systemów cyfrowych. W rozwój środowiska SMAC zaangażowani są nie tylko programiści ale antropolodzy, behawioryści, socjolodzy. Szersze cele prac nad cyfrową gospodarką, cyfrowym środowiskiem biznesowym to możliwość tworzenia inteligentnych produktów, budowanie doświadczenia biznesowego, analityka wielkich zbiorów danych, dostarczenie narzędzi badania rozwoju rynku dla producentów, dostawców i sprzedawców, przewidywanie przyszłych potrzeb klientów, tworzenie następnej generacji cyfrowych pracowników, budowa nowych interfejsów człowiek – świat cyfrowy, itp. Zaawansowana analityka biznesowa SMAC korzysta ze źródeł socjalnych, źródeł IoT, baz danych ogólnych i specjalistycznych, stosuje metody statystyczne, korelacyjne, porównawcze i inne w celu wspomagania i poprawy jakości podejmowanych decyzji biznesowych. Pakiet narzędzi i usług ICT SMAC jest oferowany przez szereg firm ICT komercyjnie jako biznesowe środowisko programistyczne i usługowe transformujące przedsiębiorstwa do zaawansowanego i rozwojowego poziomu cyfrowego kompatybilnego także z IoT. Pakiet może zawierać wiele składników jak bezpieczną komunikację, zarządzanie opinią medialną i socjalną, dostarczanie danych, poszukiwanie i kreowanie opinii, narzędzia dla komunikacyjnej warstwy mobilnej, narzędzia analityczne związane z bezpieczeństwem, tworzenie modeli biznesowych dopasowanych sektorowo do ewoluującego rynku cyfrowego, i wiele innych. Ze względu na zbieżność rozwiązań, obserwowana jest naturalna konwergencja technologii pomiędzy IoT oraz SMAC poprzez tworzenie rozwiązań I-SMAC – IoT in Social, Mobile, Analytics and Cloud (i-smac.org). Taka konwergencja jest w pewien sposób sponsorowana przez globalne organizacje standaryzacyjne działające w obszarze elektroniki i automatyki, telekomunikacji, teleinformatyki, inżynierii oprogramowania, ICT, itp., np. Instytut IEEE.

Grupa Robocza ECLIPSE IoT (iot.eclipse.org) jest zorientowaną na rozwój biznesu kolaboracją naukowo – przemysłową tworzącą otwarte, standaryzowane technologie dla aplikacji IoT. Ukierunkowanie na rozwój biznesu jest umieszczone bezpośrednio w statucie kolaboracji Eclipse definiującej IoT jako platformy transformującej sposób komunikacji jednostek i organizacji z klientami, zaopatrzeniem, partnerami i innymi jednostkami. A narzędziem do tego są połączone czujniki, aktuatory i urządzenia sieciowe umożliwiające zbieranie, wymianę i analizę generowanych danych. Proponowana architektura standardowego, otwartego oprogramowania dla IoT obejmuje trzy warstwy: urządzeń, dostępu, i chmury, oraz funkcjonalności międzywarstwowej. Dla tych warstw oprogramowania tworzone są rozwiązania referencyjne. OASIS [oasis-open.org] jest przemysłowo–naukowym, publiczno–prywatnym, technicznym i opiniotwórczym konsorcjum niedochodowym działającym na rzecz rozwoju, konwergencji i adaptacji otwartych standardów globalnego społeczeństwa informacyjnego. Opracowuje standardy dla IoT, cyberbezpieczeństwa, obliczeń chmurowych, energetyki, sieci web, itp. Celem prac jest obniżenie kosztów systemów IoT, stymulacja innowacji biznesowej, wzrost rynków globalnych, zabezpieczenie wolnego prawa przemysłu do wyboru technologii. W konsorcjum reprezentowanych jest kilkaset organizacji z ponad 60 krajów, w tym także z Polski.

Fundacja prpl (prplfoundation.org) jest niedochodowym członkowskim stowarzyszeniem przemysłowym ICT promującym rozwój i standaryzację otwartych systemów wbudowanych dla centrów danych, sieci komputerowych, oraz elementów i urządzeń dla IoT. Obecnie większość urządzeń IoT bazuje na tanich, wysoko wydajnych rozwiązaniach wbudowanych, korzystających z uproszczonych protokołów komunikacyjnych i wymagających do obsługi małych zasobów. Systemy wbudowane korzystają z procesorów MIPS, a w szczególności procesorów RISC. Obecnie najpopularniejszym stosowanym procesorem tego typu jest ARM, używany w routerach, kartach rozszerzeń standardów przemysłowych np. MTCA, a także wielu autonomicznych urządzeniach IoT. Fundacja prpl działa poprzez specjalistyczne grupy inżynierskie w takich obszarach jak emulacje procesorów, bezprzewodowe sieci komputerowe i wykorzystaniem wbudowanego systemu operacyjnego OpenWrt, wirtualizacja i bezpieczeństwo IoT. Fundacja prpl prowadzi badania konsumenckie dotyczące sposobów użytkowania urządzeń inteligentnych IoT oraz związanych z tym zagadnień bezpieczeństwa. Dostępne są bardzo wartościowe otwarte opracowania Fundacji prpl dotyczące np. bezpieczeństwa inteligentnego domu, a także obszerny raport analizujący krytyczne obszary bezpieczeństwa niezwykle popularnych systemów wbudowanych. Jako zupełnie nie śmieszny przykład z tych raportów można podać badania nad podatnością inteligentnych źródeł światła DEL Philips Hue Lightbulbs na infekcję wirusem w celu uzyskania dostępu do sieci domowej. Sieć takich 'żarówek' DEL, nie połączona bezpośrednio z Internetem, wykorzystuje do celów optymalizacji zużycia energii elektrycznej i sterowania oświetleniem nieodporny na ataki standard komunikacji bezprzewodowej ZigBee. Nie możliwy jest w tym przypadku bezpośredni atak typu DDoS, ale przejęcie kontroli nad sterowaniem wielu urządzań konsumentów energii może być potencjalnie niebezpieczne. Podawanych i katalogowanych jest wiele podobnych na ogół szeroko udokumentowanych przykładów zagrożeń wprowadzanych przez niedostatecznie zabezpieczone urządzenia brzegowe IoT. Przykłady podaje Fundacja prpl, ale także firmy analityczne, producenci, liczne newslettery IoT, jak IoTnews (iottechnews.com), organizacje ICT i IoT, a także media społecznościowe, wśród których można wymienić np. BitDefender, DataFloq, Toptal, WindRiver, Infineon, Cisco, EAI – European Alliance for Innovation, IoT Security Foundation, Gartner, TechTarget, Cybra, i wiele innych. Dane z Asystenta głosowego IoT Amazon Echo są dostępne na serwerze producenta. Mogą być dostępne dla policji, hakerów i gdzieś indziej. Amazon Echo może być wykorzystany także jako interfejs do domowych systemów IoT, np. współpracuje z urządzeniami IoT Belkin WeMo i Philips Hue. Innym robotem społecznym, asystentem domowym z poczuciem humoru jest Jibo (jibo.com), a także Kuri (hejkuri.com). Popularne ostatnio zamki cyfrowe Bluetooth są relatywnie łatwe do złamania, co pokazują przeprowadzone niedawno systemowo badania techniczne wielu takich urządzeń (Tomsguide, Cnet, Thehackernews, itp.). Bardzo podatne na złamanie są inteligentne gniazdka elektryczne, kaloryferowe urządzenia sterowania ogrzewaniem, systemy oświetleniowe, smart TV, lokalizatory, urządzania ostrzegające, itp. Przez niektóre z tych urządzeń można przejąć kontrolę nad całym brzegowym segmentem lokalnej sieci IoT. Rozmaitość stosowanych urządzeń sieciowych, bezprzewodowych i przewodowych do wyposażenia inteligentnego domu i jego otoczenia, działki, płotu, zaparkowanego samochodu, jest tak duża, i wiele z tych rozwiązań nie posiada adekwatnych zabezpieczeń do zagrożenia. Przez magistralę CAN dostępną w furtce, czy niezauważalnie uszkodzonym 'inteligentnym' lusterku samochodowym, a także poprzez ulot elektromagnetyczny, można dostać się do domowej sieci LAN. Szczególnie nieodporny na zagrożenia jest zbiór protokołów UPnP, chętnie wykorzystywany do automatycznej konfiguracji różnych funkcjonalnych urządzeń sieciowych. Fundacja prpl zwraca uwagę, że inteligentne domy nie są przyszłością, są w wielu miejscach teraźniejszością, najczęściej powstają dzisiaj ewolucyjnie poprzez wymianę ich sprzętu na 'inteligentny, i problemy związane z ich bezpieczeństwem są bardzo istotne już dzisiaj. Dla kilku najbardziej rozwiniętych krajów świata Fundacja prpl śledzi statystyki wzrostu wyposażania domów, mieszkań i firm w urządzenia inteligentne IoT i ich poziom bezpieczeństwa. Statystyki wzrostu nasycenia gospodarstw domowych IoT są okresowo publikowane. Fundacja prpl opracowuje w grupach roboczych urządzenia wirtualizujące sprzęt i dzielące sieć brzegową IoT na bezpieczne domeny.

IEEE P2413 jest projektem typu top – down realizowanym przez grupę roboczą Architektura IoT działającą wewnątrz Stowarzyszenia Standaryzacyjnego IEEE (IEEE Standards Association). Grupa robocza IEEE-SA-IoT opracowuje globalne, ontologiczne ramy architektoniczne dla IoT. IEEE jako jedna z najsilniejszych i najbardziej wpływowych organizacji naukowo-technicznych na świecie, także pod względem gospodarczym i politycznym, określa swoje działania jako transnarodowe, w związku z czym opracowania abstrahują od jakichkolwiek warunków i wpływów lokalnych. Opracowania są silnie zakotwiczone w analizie postępu naukowo-technicznego, rozwoju rynków, uwzględniając uwarunkowania społeczne i gospodarcze. Środowisko naukowo-przemysłowo-polityczne IEEE-SA-IoT, jednak ze znaczną dominacją dużego przemysłu, określa siebie samo, za przyzwoleniem

przynajmniej części adekwatnych środowisk międzynarodowych, jako takie które potrafi i powinno wprowadzić porządek na rynek przemysłowy IoT. IEEE rozpoczęło systematyczną działalność w obszarze IoT kilka lat temu (2012). Powstał portal IEEE IoT (iot.ieee.org), IoT eNewsletter, dedykowane czasopismo naukowo-techniczne, zorganizowano w Mediolanie w 2015 roku światowe forum IoT, powołano standaryzacyjną grupę roboczą, rozpoczęto budowę globalnej biblioteki przypadków zastosowania IoT, utworzono kanały społecznościowe IoT na Twitterze, LinkedIn, Flipboardzie, i Google Hangouts, opracowano szereg kursów instruktażowych wdrażania IoT w postaci webinariów, opracowano moduły e-edukacyjne do zastosowania we własnych aplikacjach IoT, wspieranych jest kilka konferencji IoT rocznie w różnych regionach świata, organizowane są cykliczne warsztaty na temat nowych technologii, zastosowań i przyszłych modeli biznesowych dla firm IoT typu spin-off i start-up i inwestorów. Platformę wyjściową do opracowania globalnego standardu architektury IoT stanowi zestaw podstawowych założeń analitycznych, obserwacja nauki, predykcja działań przemysłu i systemowa pomoc przemysłowi. Rozwój rynku IoT wskazuje na szybki wzrost liczby permanentnie usieciowionych urządzeń. Według oceny IEEE-SA, bazującej na badaniach Intela (członka IEEE-SA), ta liczba przekroczy 50 miliardów w roku 2020. Liczba okresowo podłączanych urządzeń IoT przekroczy wówczas 200 miliardów, co przy szacowanej populacji 7,5 miliarda ludzi oznacza łącznie ponad 30 urządzań IoT na osobę. Dzisiaj ta liczba wynosi ok. 10. Łączone urządzania IoT posiadają obecnie trudno standaryzowane architektury heterogeniczne, dlatego będą przedmiotem standaryzacji. W sumie generują znaczne ilości danych, wymagające zastosowana technologii Big Data i transmisji szerokopasmowej. Główne domeny aplikacyjne, które są uwzględniane w pierwszej kolejności przy opracowywaniu standardu IoT to rynek konsumenta (elektronika ubieralna, automatyka domowa, dobrobyt człowieka), rynek komercyjny (handel detaliczny, budownictwo, logistyka), przemysł (produkcja, energia, transport), sektor publiczny (inteligentne miasta i regiony, bezpieczeństwo publiczne, ochrona, opieka zdrowotna). Rynek IoT charakteryzuje różnorodność podejść biznesowych, które obejmują takie obszary jak inteligentne usługi, otwarte ekosystemy, różne ścieżki wartości, wiele rożnych stosowanych modeli biznesowych, oraz znaczna dynamika procesów cyfryzacji i usieciowienia rynku oraz pojawiania się i działania nowych aktorów na scenie biznesowej. Założeniem prac standaryzacyjnych architektury IoT jest ich silny związek z bieżącym rozwojem rynku. Na podstawie analizy rzeczywistych rynkowych przypadków zastosowania IoT, ekstrakcji z nich pewnych cech wspólnych oraz modelowania, tworzona jest biblioteka projektów odniesienia. Z rozwojem przyszłego standardu IEEE 2413 związane są dalej rozwijane i modyfikowane techniczne standardy międzynarodowe dotyczące czujników IEEE 2700, inteligentnych sieci czujnikowych i IEEE 1451, RFID, WiFi, Bluetooth, ZigBee IEEE 1902 i 802.15, komunikacji M2M IEEE 802.16, protokołów sieciowych IEEE 1888, 1855, i inne. W opracowanie standardu IEEE 2413, a więc budowy globalnego ekosystemu IoT, zaangażowane są produkcyjne i analityczne firmy amerykańskie, azjatyckie i europejskie jak np.: Broadcom, Cisco, Huawei, IBM, III – Institute for Information Industry, SEMI, Tatung, STMicroelectronics, IDC, Schneider Electric, Siemens, GE, Oracle, Toshiba, Hitachi, i inne (ieee.iot.org). IEEE w ramach standardu IoT, współpracuje bezpośrednio lub pośrednio z kluczowymi europejskimi i międzynarodowymi instytucjami badawczymi, przemysłowymi, standaryzacyjnymi, i środowiskowymi jak IETF – Internet Engineering Task Force (ietf.org), ETSI – Europejskim Instytutem Norm Telekomunikacyjnych (etsi.org), AIOTI – The European Alliance of IoT Innovation (aioti.org), Grupą Roboczą IoT Międzynarodowej Organizacji Normalizacyjnej ISO JTC1/WG10 (iso.org), IEC – Międzynarodową Komisją Elektrotechniczną (iec.ch), Konsorcjum OneM2M (onem2m.org), Grupą Studyjną IoT Międzynarodowej Unii Telekomunikacyjnej ITU SG20 (itu.int), Fundacją OPC – The Industrial Interoperability Standard (opcfoundation.org), Konsorcjum OFC, Fundacją IVI (ivifoundation.org), Koalicja IPSO – Internet Protocol Small Objects (ipso-alliance.org), Europejskim Klastrem Badawczym IoT – IERC (internet-of-things-research.eu), OpenIoT (openiot.eu), ZigBee Alliance (zigbee.org), i innymi. Wymienione instytucje opracowują standardy przemysłowe i użytkowe, sprzętowe, programistyczne, bezpieczeństwa, w szczególności, standardy komunikacyjne i architektoniczne M2M i brzegowe, stanowiące jeden z fundamentów IoT. Standard IEEE 2413 nie będzie oferować zupełnie nowej architektury IoT. Będzie silnym globalnym integratorem rozproszonych szerokich prac prowadzonych przez wymienione kluczowe instytucje i spełniającym wymagania zgłaszane przez przemysł. W celu zapewnienia odpowiedniego poziomu ogólności, skalowalności i interoperacyjności standardu IoT będzie on spełniał ściśle wymogi międzynarodowego standardu ISO/IEC/IEEE 42010:2011 dotyczącego opisu architektonicznego systemów i inżynierii oprogramowania. IEEE 2413 uwzględnia zintegrowaną, analityczną metodologię oceny ryzyka RAMS – reliability, availability, maitainability, safety. Bieżąca wersja opracowania IEEE Ekosystem dla IoT jest dostępna poprzez stowarzyszenie IEEE-SA (standards.ieee.org). W publicznych opiniach dotyczących standaryzacji IoT prowadzonej przez IEEE i inne organizacje międzynarodowe przewijają się tezy, że obecny etap prac jest ograniczony do specyficznych domen aplikacyjnych i zdominowany przez niektóre grupy interesariuszy. Oznacza to że standaryzacja objęła nie połączone sub-obszary IoT i czasami wykonywana jest w sposób niepotrzebnie nadmiarowy. Wśród tych aktywnych domen i interesariuszy IEEE-SA wymienia: media, zdrowie, logistykę, mobilność i transport, produkcję, energię, handel, oraz dom i budownictwo. Ramy architektoniczne IoT w opracowywanym standardzie IEEE 2413 będą promować interakcje między domenowe, wspomagać inter-operacyjność systemową i kompatybilność funkcjonalną, redukować fragmentację przemysłu, oraz mają być motorem dalszego wzrostu rynku IoT. Architektura powinna być budowana na rozwijanych modelach odniesienia i zapewnić przejrzystość umożliwiającą testowanie i porównywanie wydajności różnych systemów, ocenę bezpieczeństwa i stopnia pasywnej i aktywnej ochrony konsumenta.

Komisja Europejska podejmuje różne inicjatywy prawne, ekonomiczne, standaryzacyjne, i organizacyjno-logistyczne obejmujące bezpośrednio IoT, i mające na celu intensyfikację i uporządkowanie procesów budowy europejskiej E-gospodarki i Pojedynczego Rynku Cyfrowego DSM – Digital Single Market (euractiv.com/sections/digital-single-market/), także ułatwienie i przyspieszenie procesów konwersji nauka – przemysł (inter-iot-project.eu), interoperacyjności (interoperabilityiot.org). Komisja wpływa także na członków UE w kierunku cyfryzacji przemysłu, powszechnego zastosowania technologii IoT, budowy i otwarcia wspólnego rynku cyfrowego usług i dóbr. Komisja sponsoruje działania w kierunku bezpieczeństwa IoT, na przykład poprzez wsparcie dla cyklicznych dużych europejskich konferencji na ten temat, jak SaSeIoT – Safety and Security of IoT. Analizowane są przeszkody na drodze cyfrowego przekształcenia Europy, budowy e-przemysłu, otwartego e-handlu, itp. Organizowane są koalicje narodowych platform gospodarczych w obszarze Internetu, tworzona jest europejska platforma IoT, organizowane są cykliczne konferencje NetFutures na ten temat przyszłościowych aplikacji IoT, finansowane są projekty integrujące środowiska badawcze i przemysłowe. Działania, inicjatywy i projekty dotyczą konwergencji w ramach całego sektora rynku cyfrowego technologii e-marketingu, e-handlu, telekomunikacji, baz danych itp. Aktywnie działająca obecnie platforma IoT-EPI – IoT European Platforms Initiative (iot-epi.eu) koordynuje finansowanie europejskie w obszarze IoT, w tym uruchamia projekt H2020 BIG-IoT - Bridging the Interoperability Gap of the Internet of Things (big-iot.eu). Projekty EPI dotyczące IoT o znacznym łącznym finansowaniu obejmują obecnie: symbIoT, bIoTope, AGILE, VICINITY, TagItSmart, interIoT. Celem tych pan-europejskich projektów jest implementacja dwóch wspólnych wysoko standaryzowanych technologii IoT w Europie, wspólnego interfejsu użytkowego API oraz wspólnego rynku, i przez to budowa sprawnego europejskiego ekosystemu IoT. Europejski ekosystem IoT powinien charakteryzować się interoperacyjnością międzyplatformową i międzysystemową (symbIoTe), łatwością implementacji w przedsiębiorstwie, i niskimi kosztami inwestycyjnymi (bIoTope), modularnością na poziomie sprzętowym (AGILE), wspólnym interfejsem API (BIG IoT), standaryzacją komunikacji M2M (VICINITY) oraz interoperacyjnością jako usługą, możliwością znakowania i śledzenia produktów na rynkach masowych (TagItSmart), oraz umożliwiać wspólne sprawne działanie heterogenicznych systemów IoT w przypadku jeszcze ciągłego braku standardów globalnych (interIoT).

Międzynarodowa, raczej trzeba byłoby powiedzieć globalna, przestrzeń polityczno-gospodarczo-organizacyjna IoT i cyfryzacji gospodarki, oraz transferu technologii IoT nauka – przemysł, jest jeszcze znacznie bardziej skomplikowana i bogatsza niż wynikałoby z powyższego opisu działania wymienionych licznych organizacji i podejmowanych przez nie działań. Organizowane są międzynarodowe platformy dyskusyjne, jak np. IoT Forum (iotforum.org). Wiele działalności profesjonalnych IoT koordynuje Europejski Klaster Badawczy IoT IERC (internet-of-things-research.eu). Organizowanych jest kilka kluczowych cyklicznych konferencji IoT o charakterze globalnym, jak np. IoT-week (iot-week.eu), IoT Tech Expo (iottechexpo.com), któ-

rych podsumowanie można znaleźć na otwartej stronie agregacyjnej iotevents.org. W rozwój IoT zaangażowane są rządy, wojsko, wielki biznes, przemysł, tysiące małych i średnich firm, szeroki rynek konsumpcyjny, także szara strefa gospodarcza, itp. Niektóre z dużych organizacji gospodarczych mają także ambicje dołożyć się do przewidywań rozwoju rynku IoT, budowy narzędzi analitycznych i szerszych opracowań dotyczących rozwoju infrastruktury i standardów IoT oraz IIoT. Analizy sektorowe, środowiska programistyczne i opracowania takie powstają jako osobny, równoległy nurt do działania organizacji rządowo-gospodarczych, konsorcyjnych i społecznościowych. Obejmują one kilka obszarów jak np. uaktualniane, komercyjne ekonomiczne środowiska analityczne (Eikon, Bloomberg Terminal, Forbes, itp.) obecnie zaczynające także korzystać ze źródeł IoT, komercyjne wieloaspektowe analizy rozwoju rynków wysokotechnologicznych, analizy wąsko-sektorowe IoT na zamówienie, ogólniejsze opracowania opcji architektur IoT z punktu widzenia interesu wybranych sektorów gospodarczych. Można zauważyć kilka cech charakterystycznych takich środowisk analitycznych i opracowań dotyczących IoT. Analizy rynków on-line w czasie rzeczywistym i wyprzedzające zaczynają intensywnie korzystać z danych generowanych przez IoT (IoT Analytics, Accenture, PTC, Vitria, Tellinet, AGT International, TechTarget, IDC Analysts, Opto22, i wiele innych). W przekrojowych sektorowych, a także ukierunkowanych opracowaniach statycznych i dynamicznych, dane IoT uzupełniają analitykę konwencjonalną stosowaną do tej pory. Niektóre opracowania, oprócz oferowanych narzędzi, zawierają różne rodzaje tutoriali i kursów wirtualnych, oraz praktycznie zorientowanych webinariów jak interpretować i korzystać z danych IoT do efektywnego rozszerzenia analityki biznesowej (opto22, tellit). Dostępne instrukcje wspomagające konwersję dotyczą także sposobów zarówno minimalno-inwestycyjnej jak i poważniejszej systemowej rekonfiguracji firmowych zasobów komputerowo – sieciowych pozwalających na wchłonięcie danych IoT przez własny firmowy system analityczny. Intel oferuje specjalistyczne kompleksowe rozwiązania sprzętowe dla takich celów. Na bazie procesorów i mikrokontrolerów ARM, Intela i innych producentów, wiele firm oferuje różne kompleksowe rozwiązania sprzętowo – programistyczne dla wielofunkcyjnych aplikacji IoT. Opracowania architektoniczne IoT przygotowywane przez niektóre firmy ICT mimo wielu podobieństw są nieco odmienne od działań standaryzacyjnych opisanych poprzednio. Są bardziej ukierunkowane na praktykę i bliższy horyzont czasowy. Zapewne kiedyś wiele obserwowanych kierunków działań doprowadzi do kompromisu, na którym wszyscy skorzystamy. Warto jednak zauważyć, że trzeba mieć odwagę dzisiaj z występowaniem z własnymi firmowymi rozwiązaniami architektonicznymi w przypadku globalnego, otwartego zaangażowania tak znacznych zasobów intelektualnych i technologicznych. Rynek IoT jest ewidentnie w stanie przejściowym, turbulentnym, dynamicznej budowy i ciągłej rekonfiguracji (Kranz 2016).

Człowiek a IoT

Mówi się, że IoT to głównie pod względem masywności transportu danych oddziaływanie między maszynami M2M (Holler 2014), (Armstrong 2016), (Chen 2017). Jednak zaczynamy od ważniejszej dla nas obecnie relacji człowiek – IoT (Leonhard 2016). To ta relacja zdecyduje o dalszym rozwoju usługowego i przemysłowego IoT. Jeśli ta relacja pójdzie w złym kierunku, nie wiadomo jak ten rozwój potoczy się dalej. IoT zostanie tylko domeną maszynową? To wydaje się niemożliwe. Człowiek oddziałuje z IoT w złożony sposób, a także IoT oddziałuje z człowiekiem. Jakie są niektóre argumenty, czynniki, atrybuty, konsekwencje, zachodzące procesy określające to oddziaływanie? Można nieco arbitralnie i w sposób nieuporządkowany wymienić: czas, odległość fizyczną i psychologiczną, interfejsy, poznanie wzajemne, akceptację, przyzwyczajenie, powstające pokolenie cyfrowe, zależność od IoT, nowe prawo pisane i niepisane, działalność, itp. IoT zorientowane na człowieka obsługuje takie obszary jak zdrowie, transport, inteligentne miejsce zamieszkania, przyjazne miasto, stanowisko pracy, działalność gospodarcza człowieka, ochrona środowiska dla człowieka, bezpośrednie bezpieczeństwo człowieka i otaczającej go przestrzeni. Jeśli założymy że najważniejsza jest praca, to IoT wkrótce całkowicie zmieni wiele z naszych stanowisk pracy, wprowadzając dodatkową, istotną różnorodność. Jeśli założymy że najlepszym czasem człowieka jest ten spędzony z rodziną, na aktywnym wypoczynku, dbaniu o zdrowie, i w twórczej pracy, to inteligentna infrastruktura, czyli IoT ma redukować czas człowieka spędzany na innych czynnościach – zakupy, sprzątanie, prace uciążliwe, prostsza praca która łatwo podlega automatyzacji, a w przyszłości praca znacznie bardziej skomplikowana. Na nowym stanowisku pracy wspomaganym przez IoT i AI spotkamy się z zagadnieniem akceptacji i przyzwyczajenia się do rozszerzenia naszych możliwości twórczego działania. Nasz zespół zadaniowy w pracy będzie prawdziwie hybrydowy ludzko – maszynowy, w tym sensie że maszyna nie da się zepchnąć do roli biernego podpowiadacza rozwiązań, czy tylko mechanicznego wykonawcy zadań. W nowym miejscu pracy, obszarze współpracy intelektualnej z człowiekiem przez nową kategorię pracowników, zamiast terminu maszyny zaczęto używać terminu nieludzie – nonhumans (baldfuturist.com). Nieczłowiek, nieludzie będą prawdziwymi partnerami człowieka w pracy. Jeśli człowiek jest związany z IoT poprzez czas to także poprzez odległość. Można nieco w przenośni i przewrotnie powiedzieć, że od tej odległości zależy sposób interakcji człowieka z IoT. Dystans ten wydaje się być coraz mniejszy, nie wiadomo czy nie dąży do zera. IoT nas dotknie bezpośrednio, naszego ciała i umysłu. W kilku obszarach IoT jest bardzo bliski człowieka: czujniki w jego otoczeniu, interfejsy osobiste, ciągle jeszcze kontrowersyjne osobiste bazy danych „na zawsze" – jak np. EterniMe, wyniki działania i sfera informacyjna ukierunkowana na osobę. W pozostałych powinien być niewidoczny. Interakcja w obie strony jest niesymetryczna. Człowiek naturalnie chce decydować o wszystkim, ale to nie ma sensu. Wiele decyzji odda inteligencji IoT. Mało tego. To IoT będzie obserwować człowieka, poznawać swojego użytkownika – jego zachowanie, stan emocjonalny, w przyszłości mierzyć ulot elektromagnetyczny i biochemiczny, schematy zachowań. Bardziej inteligentny IoT znacznie lepiej pozna zwyczaje użytkownika. Wszystko to uczyni życie człowieka zupełnie innym, głęboko dotykając naszej osobowości i chyba pozostanie z nami na dłużej. Będziemy podlegać transformacji cyfrowej. Pierwsze generacje „rodowitych cyfrowo" ludzi mamy pod bokiem. To są nasze dzieci, a jeszcze bardziej wnuki. Nie bez sensu jest pytanie zadane ostatnio w prasie fachowej IEEE dotyczące asystenta IoT Kuri 'Czy robotyczne nianie powinny wychowywać nasze dzieci?'. Co to oznacza dla IoT? To pokolenie, jeszcze nie całkiem wirtualne, ale już jest elementem dodatniego sprzężenia zwrotnego w rozwoju inteligentnego otoczenia człowieka, i ewolucyjnej zmiany samego człowieka. Ta część IoT, która jest najbliżej człowieka, dotyka go bezpośrednio lub można jej dotknąć jest nazywana czasami Internetem Dotykowym – tactile – TI i IoTT.

Czy człowiek musi oddziaływać z IoT? Można byłoby postawić dzisiaj już średnio odważną, bo dobrze przewidywalną, ale mimo wszystko jeszcze nieco futurystyczną tezę, że właściwie nie. Albo przynajmniej jak najmniej. Lepiej aby IoT był niewidzialny, milczący, ale inteligentny i pomocny, bezpieczny i przyjazny, sprawny i intuicyjny. W skrócie, aby nie zawracał nam nadmiernie głowy i robił co do niego należy! Interfejs człowieka do IoT jest jednym z licznych zagadnień którymi w sposób formalny, naukowy i techniczny, zajmuje się wiele organizacji a wśród nich IEEE Society on Social Implications on Technology - SSIT. Bez wątpienia technika porywa umysł człowieka i zainteresowanie społeczeństw. Za tą fascynacją stoi poważny argument wspomagania przez technikę poznania, a za tym rozwoju społeczeństwa i człowieka. Jeśli za kryterium oceny przydatności przyjmiemy to co mamy najwartościowsze w życiu jednostki czyli czas, powracamy znowu do czasu, to obecnie nie jest najlepiej. Technika, zamiast coraz mniej według postawionej tezy, zajmuje nam coraz więcej czasu. Niektórzy są tym zachwyceni, liczni ale nie wszyscy. Ale jeszcze tak naprawdę w prawdziwą niewolę techniczną nie wpadliśmy, dopiero wpadniemy. Specjalistów, obeznanych z techniką socjologów i psychologów a także medyków, od frustracji częściowo ratuje nadzieja że jesteśmy na początku rozwoju inteligencji infrastrukturalnej. I kiedyś przyjdzie czas uwolnienia człowieka z niewoli technicznej, gadżetów, inteligentnych urządzeń, pilotów, haseł, itp.? Czy rzeczywiście? Tego nie wiemy i odpowiadanie na to pytanie to domena wybitnych umysłów futurystycznych klasy Lema. Być może, co jest bardzo prawdopodobne, będziemy popadać w coraz większą zależność, aż do jakiejś formy integracji i budzącego obecnie, ale czy na zawsze, wielkie kontrowersje moralne transhumanizmu. Transhumanizm będzie rozwijany np. w celach militarnych. Nie ma co do tego wątpliwości. Czy także pomoże w rozwiązywaniu problemów medycznych, przy pomocy implantów IoT? Oczywiście że pomoże. Budowane są protezy, neuroprotezy i inteligentne ortezy kończyn. Testowane są egzoszkielety i neuro-egzoszkielety. Testowane są sterowane implanty mięśniowe, neurologiczne, mózgowe.

Dzisiejszą bramką człowieka do IoT jest interfejs. W przyszłości będzie tylko sama jego obecność. Nie do wszystkich usług IoT potrzebny jest jakiś rodzaj interfejsu. Obecnymi interfejsami człowieka do IoT jest inteligentny zegarek i jego pasek, smartfon, okulary, tablet, laptop, komputer stacjonarny, telewizor, coraz bardziej standaryzo-

wane interfejsy RFID do systemów typu inteligentny dom, inteligentny samochód, inteligentne miasto. E-paski zegarka, a jest ich wiele dostępnych w wersjach komercyjnych i badawczych, takie jak np. Angel Wristband, Jawbone, Lenovo VibeBand, Misfit Shine, Healbe GoBe, Nebu Razer X, E Fun NexOne, i inne są wyposażone w wiele czujników, także odczytujących dane fizjologiczne z potu. Technika idzie w kierunku standardowego, spersonalizowanego interfejsu osobistego o coraz większej integracji z człowiekiem, np. biometrycznego. Taki interfejs jest wykonany w technologiach elektromagnetycznych, a kiedyś niewykluczone że będzie w biologicznych. Specjalizowane interfejsy dostępowe, ale także inne elementy systemu IoT są związane z ubraniem człowieka lub czujnikami umieszczanymi, np. tatuowanymi bezpośrednio na skórze, także aktywne soczewki kontaktowe. Bardzo duży potencjał aplikacyjny posiadają soczewki kontaktowe wyposażone nawet w matrycę tysięcy czujników, medycznych, behawioralnych, obrazowych. Zaawansowany projekt w tym kierunku prowadzi Google. Soczewki dla cukrzyków badane w Oregon State University, wykorzystujące przezroczystą elektronikę IGZO (InGaZnO), mierzą np. poziom glukozy we krwi, poprzez pomiar filmu łzowego. Wiele innych parametrów może być mierzonych w przyszłości z łez. Wśród wielu rodzajów rozwijanych dzisiaj interfejsów są urządzenia mobilne i stacjonarne, głosowe, wideo, behawioralne, intuicyjne, związany tylko z obecnością człowieka, z gestami specyficznymi lub rozpoznawanymi, zachowaniem, RFID, w samochodzie typu HUD z wyświetlaniem na szybie. Ubranie, najbliższy przyjaciel człowieka z bielizną przylegającą do naszej skóry jest łakomym obszarem dla IoT. IoT nie ma respektu dla nagości człowieka. Nie ma respektu co do penetracji jego ciała. W tą sferę intensywnie ingeruje Internet Przedmiotów. Początkowo jest to wyposażenie dla wojska oraz w cywilu dla osób niepełnosprawnych i monitorowanych pod względem zdrowotnym. Internet przedmiotów dotyka skóry człowieka, na której przyklejane lub lepiej na której tatuowane są czujniki. Soczewki kontaktowe mogą wyświetlać treść na siatkówce. Z oczujnikowaniem ubrania i skóry związanych jest szereg problemów badawczych i technicznych jak elastyczna elektronika, jej odporność na zużycie, mycie, pranie, tarcie, wygięcia, rozciąganie, itp. Są to wymagania bardzo trudne do spełnienia, ale prace nad elektroniką rozciągliwą, elastyczną i odporną są prowadzone w wielu laboratoriach. Badania prowadzą docelowo do wytworzenia elektronicznych tekstyliów z drukowanymi lub wbudowanymi w strukturę materiału układami analogowymi i cyfrowymi. Tekstylia elektroniczne są gdzieniegdzie nazywane tekstronicznymi. Są także firmy w kraju zajmujące się tą tematyką jak Intellimotion. W pewnym sensie są to badania analogiczne do prac nad elektronicznym papierem. Czujniki i elementy IoT są integrowane na ciele i na inteligentnym ubraniu człowieka, także na tradycyjnej biżuterii, w postać pełnej sieci funkcjonalnej, nazywaną siecią obszaru ciała BAN – body area network, także body access network. Funkcje takiej sieci mogą być bardzo szerokie jak kontrola dostępu, monitorowanie stanu organizmu, lokalizacja, komunikacja, rozpoznawanie, bezpieczeństwo, wspomaganie funkcji organizmu, współdziałanie z pełnym lub częściowym egzoszkieletem, współtworzenie rozszerzonej rzeczywistości, itp. Obecnie prowadzone są eksperymenty z relatywnie prostymi elastycznymi funkcjonalnymi układami elektronicznymi integrowanymi z ubraniem lub naklejanymi na skórę człowieka w różnych miejscach. Nad technologią ubrań inteligentnych pracuje wiele nowych firm technologicznych, ale także np. firma Google w ramach projektu Jacquard. Kurtka Levi's Commuter Trucker posiada duże funkcjonalne obszary dotykowe na rękawach czułe na wielodotykowe gesty użytkownika pozwalające na sterowanie wieloma funkcjami smartfonu, w tym także na odbieranie rozmów telefonicznych. System elektroniczny kurtki składa się z elektroniki zintegrowanej z materiałem i dołączanego modułu Bluetooth do zasilania i łączenia ze smartfonem. Pseudo-tatuaż elektroniczny naklejany na palcu czy na dłoni jest np. interfejsem do lokalnego systemu komputerowego i IoT poprzez gesty. Częściej pseudo-tatuaże, lub e-tatuaże służą do monitoringu parametrów fizjologicznych człowieka, a także do identyfikacji w systemie. Rozwój e-tatuaży idzie w kierunku miniaturyzacji, zmniejszenia zapotrzebowania na moc, zwiększania funkcjonalności i rodzajów oraz liczby detekowanych sygnałów jak kierunek i położenie, zbliżenie, dotyk, nacisk, rozciągnięcie, drgania, dźwięk, siła ściskania, miejsce dotyku, spocenie, temperatura, przyspieszenie. W sieci dostępne są opisy zarówno rozwiązań prototypowych jak i komercyjnych: SkinMarks, jSkin, DuoSkin, Skintillates, e-skin, e-tattoo, e-ink-tattoo, BioStampRC, BioStampMD, SkinPatch, WiSP Cardiac ECG, i inne. Nad inteligentnym tatuażem elektronicznym, czyli elektroniką i mechatroniką naskórkową, a także elektroniką ubieralną, pracują takie firmy jak np. Motorola, MC10 (mc10inc.com), również kosmetyczne jak L'Oreal. Obecnie oprócz coraz bardziej zaawansowanych sieci czujnikowych na skórze człowieka może być naklejony układ o podstawowej funkcjonalności komputera PC.

Warto jeszcze kilka słów poświęcić specyficznemu, chyba najważniejszemu współczesnemu interfejsowi człowieka 'do wszystkiego', także do Internetu i IoT, do innych ludzi, do biznesu, do banku, do swojego zdrowia, czyli smartfonowi i telefonii komórkowej, a na marginesie inteligentnemu telewizorowi. Inteligentny telefon łączy w sobie wiele elementów IoT. Najbardziej zaawansowane telefony mają wbudowanych dzisiaj nawet kilkadziesiąt, a wkrótce setki czujników. Część z tych czujników nie musi być umieszczona bezpośrednio w telefonie, ale łączy się z zegarkiem nareczynym, opaską zegarka, okularami, obuwiem, fragmentami garderoby. Jakie parametry smartfon i jego satelity czujnikowe mierzą dzisiaj, niektóre w rozwiązaniach testowych, a niektóre w komercyjnych: tętno, nasycenie krwi tlenem, zmęczenie, stres, potliwość, pH krwi, ciśnienie krwi, wysiłek bieżący i okresowy, pozycję osoby, rodzaj ruchu, i inne. W niedalekiej przyszłości tych parametrów będzie znacznie więcej, np.: zawartość niektórych substancji fizjologicznych i chorobotwórczych w pocie i oddechu. Zaawansowane smartfony są wyposażone w pewnym sensie antropogenny video system orientacji przestrzennej, nie tylko korzystającej z GPS, np. taki jak Google Tango. Po prostu telefon wie gdzie jest korzystając z technik uczenia się otoczenia i śledzenia ruchu, percepcji głębi, oraz porównywania obrazów widzianego i z bazy danych map i Google Streets. Wyposażenie smartfonu czy phabletu w zestaw dodatkowych czujników, orientację GSM i wi-fi, aplikację Tango i rozbudowane funkcje multimedialne zaciera różnice pomiędzy obrazem rzeczywistym i wirtualnym. Aplikacja Tango jest już dostępna także u nas w kraju. Jak może wyglądać przyszły smartfon – niedługo jak przezroczysta cienka tafla szkła, a w wersji elastycznej być może jak długopis, rozwijany do postaci kilkunastocentymetrowej kartki grubszego papieru, w dalszej przyszłości raczej będzie to obiekt silniej zintegrowany z organizmem człowieka. Nie będzie to smartfon, a raczej biocybernetyczny interfejs do sieci globalnej. Smartfon wyposażony w żyroskopy i akcelerometry, także w lokalizator i czujniki położenia pozwala na uruchomienie na nim wielu aplikacji IoT zorientowanych na użytkownika. Aplikacja 'jakość snu' wykorzystując dane z czujników i bazy danych długotrwałych pomiarów mierzy, oprócz czasu trwania i ewentualnych przerw, czas i częstotliwość fazy REM snu. Na tej podstawie określa wiele innych fizjologicznych, obiektywnych i subiektywnych parametrów snu, jak jakość, poczucie wypoczęcia. Stres jest także określany z pomiarów oraz z bazy danych która jest wykorzystywana do nauczenia smartfonu zwyczajów użytkownika. Warunkiem jest aby smartfon, czyli osobisty interfejs IoT, był cały czas z nami. Inaczej mówiąc abyśmy pozwolili mu nas śledzić i potem podpowiadać co mamy robić np. aby być zdrowym i w dobrej formie. Smartfon może budować bazę danych naszego stylu życia, zachowania, odżywiania, snu, wysiłku fizycznego i jego rodzaju, jeśli niektóre części takiej bazy systematycznie uzupełniamy. Niektóre dane są wprowadzane autonomicznie. Ze smartfonami powiązane są coraz częściej zegarki inteligentne smartwatche. Występują także w rozwiązaniach autonomicznych zawierając również funkcje telefoniczne. Wiele dostępnych rozwiązań służy do celów sportowych i zdrowotnych, także bezpieczeństwa. Mierzą nie tylko wysiłek fizyczny ilościowo i jakościowo, także reakcję organizmu, lokalizują i mapują ruch, planują zadania ruchowe i wysiłkowe. Bransolety i obrączki np. Moov Now, Kaa, Seebo, itp. mierzą kilka parametrów ruchu i reakcji organizmu i zapisują je do prozdrowotnej bazy danych w chmurze. Dostępnych jest wiele rozwiązań ubieralnych w postaci zegarków sportowych, jak Garmin, Samsung, opasek na tułów, udo i podudzie. Zegarek Calmean jest specjalnie zaprojektowany do zabezpieczenia, lokalizacji i komunikacji z dzieckiem. Oprócz dokładnego lokalizatora i telefonu zawiera kilka czujników np. sygnalizujący fakt zdjęcia zegarka z ręki, wyjścia poza obszar zdefiniowany, przycisk SOS, itp. Skarpetki Owlet Smart Sock 2 dla niemowlaków są wyposażone w czujniki mierzące tętno, utlenowanie krwi, jakość snu i przesyłają dane na telefon komórkowy rodziców.

Nie zapominamy o najważniejszej funkcji, smartfon jest interfejsem głosowym o znacznych możliwościach, interfejsem głosowym użytkownika do IoT. Interakcje głosowe są testowane np. przez pionierski system Alexa Amazon, przez Samsung Voice dla swoich telewizorów i telefonów, także Google Home i inne. Projekt Google Motorola Ara stanowi element poszukiwań zupełnie innego podejścia do smartfonu. Telefon jest składany przez użytkownika jak klocki Lego. Bardzo przyjazny interfejs głosowy jest silnie zorientowany na indywidualnego człowieka. Jest jedynie kwestią czasu przyzwyczajenie

się do wygodnych nowych możliwości i wkomponowanie ich na stałe w życie codzienne. Interfejs głosowy, jeśli nabierzemy do niego dostatecznego zaufania, będzie używany powszechnie w życiu codziennym indywidualnie, ale i we wspólnym otoczeniu człowieka, także biznesowym. Głosowo będziemy zamawiać zaopatrzenie, zamawiać usługi grupowe, zwoływać telekonferencje, sterować urządzeniami w otoczeniu, i wiele innych. Fundamentalny aspekt społeczny głosu odgrywa tutaj podstawową rolę i to zostanie bardzo szeroko wykorzystane w IoT i jego interfejsie z człowiekiem. Wszechobecny, rozproszony, zlokalizowany nie tylko w smartfonie ale w domu, w biurze, uczący się interfejs głosowy zmieni otoczenie prywatne i biznesowe człowieka. W takiej sielskiej wizji grozę budzą np. ostatnie doniesienia prasowe na temat narzędzi wykorzystywanych, nie wiadomo czy legalnie, przez służby specjalne, do podsłuchiwania i obserwacji ludzi poprzez obecne wszędzie urządzania IoT, w tym smartfony, kamery nadzoru, urządzenia bezpieczeństwa, telewizory. Jeśli ktoś z czytelników miał okazję odwiedzić laboratoria największych firm produkujących telewizory to mógł zobaczyć modele które są przygotowywane na rynek za kilka lat, w tym telewizory przezroczyste. Podobnie jak wymienione poprzednio smartfony przezroczyste. Cały wyświetlacz TV jest przezroczysty, jak tafla szkła w oknie, oczywiście gdy jest wyłączony, z niewielkim paskiem elektroniki na dole, lub elektronika jest osobno w małym panelu do interfejsów. Interfejs głosowy, rozpoznawanie gestów, obserwacja i uczenie się zwyczajów użytkownika, interfejs behawioralny, to standardowe wyposażenie tych modeli. W zależności od zwyczaju, wchodzimy do pokoju, siadamy z filiżanką kawy, telewizor odpowiednio reaguje, włączając stosowny program, przeglądarkę, edytor graficzny, muzykę, komunikator dołączający do naszej kawy kilku innych użytkowników, wygaszacz ekranu w postaci ulubionej sekwencji obrazów impresjonistów, przegląd e-prasy, lub po prostu dodatkowe oświetlenie pokoju. I to wszystko w przyszłościowej rozdzielczości 6K, 12K, na którą pozwala już dzisiaj praktycznie nieograniczone pasmo nowej generacji szkieletowych transmisyjnych sieci optycznych. A jest to tylko jedna z możliwości rozwoju telewizji IoT. Inną należy wymienić, jeszcze bardzie atrakcyjną, jeśli opanujemy dostatecznie dobrze holografię pod względem praktycznym, i stanie się to opłacalne. Tak czy inaczej, szklane czy organiczne, przezroczyste czy holograficzne ściany w naszych pomieszczeniach, biur i mieszkań powinny dać, i dadzą wcześniej niż się tego spodziewamy, poczucie pełnego zanurzenia w rzeczywistości wirtualnej. Jeszcze jednym elementem interfejsu człowieka do IoT, związanym ze smartfonem, telewizorem, komputerem, ale także samochodem i domem, jest system operacyjny. Dzisiejszym liderem w konkurencji systemów operacyjnych dla IoT jest Android obsługujący coraz sprawniej wiele urządzeń, w tym inteligentne telewizory. Konkurencja jest jednak spora: IoT Windows, OS Apple, OSTV, Tizen, Predix, itp. Żaden z nich, można być pewnym, jeszcze nie spełnia wymogów przyszłości. Prace są prowadzone w kierunku opracowania standardu uniwersalnego systemu operacyjnego dla IoT. Nie będzie to pojedyncze rozwiązanie. Inny system jest potrzebny dla człowieka, przeciętnego użytkownika, operatora, a zupełnie inny dla systemów M2M, IoT B2B, itp. System operacyjny IoT pośredniczy pomiędzy rozwiązaniami i aplikacjami IoT a chmurą oraz fizyczną i wirtualną bramą do obszaru brzegowego IoT, i dalej poprzez różnorodne standardy techniczne akwizycji, cyfryzacji i transmisji danych do urządzeń sprzętowych.

Rozszerzona rzeczywistość AR – augmented reality, zamiennie nazywana, jednak w nieco innych znaczeniach technicznych, wirtualną, komputerowo wspomaganą, symulowaną, mieszaną, modulowaną, pośredniczącą, tworzona wokół człowieka i wykorzystywana przez niego, stanie się praktyczną codziennością. Rzeczywistość rozszerzona jest także rodzajem interfejsu człowieka do IoT. Rzeczywistość rozszerzona jest już częściowo, a będzie coraz szerzej stosowana w kontaktach biznesowych, wspomaganiu zakupów, kursach jazdy samochodem, na nartach, rozrywce i planowaniu urlopu z testową wirtualną osobistą wizytą w miejscu, z atrybutem pełnego zanurzenia w otoczeniu. Rozszerzona rzeczywistość, szczególnie taka w wersji częściowego zanurzenia, łącząca rzeczywistość realną z wirtualną, będzie miała ogromny wpływ już niedługo na sposób działania biznesu, pozwoli na nowe innowacyjne sposoby zakupu i sprzedaży produktów i usług, zmieni relacje sprzedawca – klient. W dniu dzisiejszym rozwiązania AR pozwalają na zbieranie doświadczenia w funkcjonalnym łączeniu różnych warstw rzeczywistości w celu kreowania nowych funkcjonalności. Szczególnie istotna jest warstwa wspomagania decyzji człowieka korzystającego z systemu AR, wspomagana intuicyjnie selekcjonowanymi i dostarczanymi danymi IoT. W systemie AR obecni są wirtualni asystenci człowieka. Działają skutecznie już obecnie jak: Siri, Cortana, Google Now, Google Allo, Alexa. Wirtualni asystenci zmieniają sposób w jaki szukamy produktów i usług. Coraz częściej klienci używają asystentów wirtualnych na urządzeniach mobilnych zamiast nawigować w wyszukiwarkach internetowych smartfonów, maszyn mobilnych i stacjonarnych. Ten trend jeśli zostanie utrwalony całkowicie przekształci reklamę i przemysł marketingowy. Dostępne aplikacje i urządzenia rzeczywistości rozszerzonej obejmują np. okulary i hełmy wspomagające widzenie w warunkach przemysłowych, okulary dla straży pożarnej dodające obraz podczerwony, kamery IR i wyświetlacze wzmocnionego obrazu na przedniej szybie samochodu, liczne aplikacje na smartfony wyświetlające kontekstowo znaczne ilości dodatkowych, przydatnych informacji, aplikacje telemedycyny, interfejsy zdalnego doradztwa eksperckiego, aplikacje robotyczne, sklepy wirtualne, salony sprzedaży, biura wirtualne, systemy zarządzania kontaktami z klientami, i wiele innych. Dla zilustrowania tempa rozwoju zastosowań IoT rzeczywistości wirtualnej obsługującej człowieka warto wymienić kilka przykładów funkcjonalnych urządzeń komercyjnych: kamizelka dotykowa, cyber-rękawice żyroskopowe, okulary Google, okulary Microsoft HoloLens, okulary Samsung, LeapMotion bezdotykowy układ śledzenia ruchów ręki i palców, Kinect układ śledzenia ruchu, Razer Hydra, AlloSphere, Cave i TreadPort – pokoje wirtualne, ARToolKit – otwarte środowisko programistyczne rzeczywistości rozszerzonej. E-okulary będą jednym z bardzo ważnych interfejsów człowieka do świata IoT. Obecne rozwiązania komercyjne np. Lumus of Rehovot, DeepOptics, MobilEye, i inne, są oferowane do tworzenia AR i praktycznego wykorzystania w logistyce, gospodarce magazynowej, bezpieczeństwie ruchu drogowego, rozrywce, itp. Technologie wykorzystywane do budowy przestrzeni rzeczywistości rozszerzonej obejmują, między innymi: grafikę komputerową, modelowanie i rendering wideo, systemy wizyjne swobodnego punktu widzenia, systemy ruchu omni-kierunkowego, holografię, i inne.

Wspominano już poprzednio, że świat IoT generuje nowe pojęcia jak cyfrowe bliźniaki, odpowiedzialność, moralność, prawo w świecie wirtualnym. Termin cyfrowy bliźniak zaczął funkcjonować w literaturze inżynierii Internetu ok. trzy lata temu, choć dotyczy zagadnienia inaczej nazywanego nad którym nauka pracuje znacznie dłużej (Smart 2014), (Volkmann 2016). Termin zawiera trzy różne kategorie cyfrowego odzwierciedlenia, z jednej strony przedmiotu, urządzenia, systemu, i z drugiej strony realnego człowieka, mnie, ciebie, oraz osoby elektronicznej – biobota nie będącego odzwierciedleniem konkretnego człowieka. W pierwszym przypadku chodzi o coś znacznie więcej niż deterministyczną maszynę stanu odzwierciedlającą obserwowany system. Powinien to być model systemu pozwalający dokładnie odzwierciedlić jego stany normalne i anomalne w przyszłości we wszystkich warunkach pracy, także stany przejściowe. W drugim przypadku jest to coś znacznie więcej niż mój własny bot, czy kilka botów którymi posługuję się w sieci. Coś znacznie więcej niż prosty prototyp bliźniaka takiego jak Cortana Microsoft. Docelowo to powinienem być ja, wirtualny ja, jak najdokładniej ja, ze wszystkimi moimi atrybutami, myśleniem, zachowaniem, emocjami, przyzwyczajeniami, itp. Niektórzy analitycy wirtualnej rzeczywistości nadają takiej osobie dodatkową rolę Anioła Stróża, korzystając z faktu że taka wirtualna osoba posiada dostęp on-line do znacznie większej ilości danych i znacznie szybciej je analizuje niż realny człowiek. W trzecim przypadku chodzi o człowieka elektronicznego (poprzednio nazwanego nieczłowiekiem), działającego w przestrzeni wirtualnej wykwalifikowanego pracownika wykonującego pracę rzeczywistych ludzi. Mówi się czasami o niewolnikach cyfrowych, bowiem wyposażonych w świadomość. Wymienia się wielką rozmaitość cyfrowych towarzyszy człowieka, inaczej bio-boty IoT zorientowane na człowieka, boty wdrażające nowego pracownika w korporacji, boty pomagające w zakupach, służbie zdrowia, warsztacie samochodowym, w turystyce, boty związane z bezpieczeństwem, rozrywką, towarzysze człowieka w świecie wirtualnym, czy przyjaciele? W pierwszym przypadku chodzi o budowę sieci cyfrowych bliźniaków rzeczy będących zwierciadlanym odbiciem Internetu Przedmiotów, takiego jak go dzisiaj rozumiemy. W drugim i trzecim przypadku chodzi o stworzenie bliźniaczego modelu społeczeństwa z wielowarstwowej sieci połączeń pomiędzy cyfrowymi bliźniakami ludzi rzeczywistych i ludzi całkowicie wirtualnych. Wszystko to obiekty cyfrowe, w przyszłości niektóre z nich prawdopodobnie w jakimś stopniu samoświadome. Nic nie stoi na przeszkodzie aby zbudować pomiędzy tymi warstwami odpowiednie interfejsy. Mówiąc nieco w przenośni, wirtualną warstwę rzeczy nasycimy inteligencją ludzką, wirtualną warstwę ludzką wyposażymy w dodatkowe zmysły i możliwości wykonawcze. Ograniczając się do warstwy rzeczy, nie będzie jednej inteligentnej infrastruktury cywilizacyjnej, lub jak dzisiaj nazywamy jednego Internetu

Przedmiotów, tego rzeczywistego. Będzie przede wszystkim wiecznie doskonalony model infrastruktury cywilizacyjnej, obserwujący rzeczywistość, ciągle uczący się, obserwujący rozbieżności w procesach modelowych i rzeczywistego rozwoju i budowy cywilizacji i optymalizujący procesy, miejmy nadzieję zgodnie z życzeniem ludzi. Nauka już doskonale zdaje sobie sprawę, że mniej więcej taki będzie kierunek rozwoju inteligencji infrastrukturalnej IoT oraz wirtualnego świata bliźniaczego i ich współdziałanie z rzeczywistym światem ludzi. Prowadzona jest dyskusja nad moralnością maszynową na obecnym etapie początkowego rozwoju inteligencji maszynowej. Dotyczy to problemu oddania odpowiedzialności za mienie znacznej wartości, a także zdrowie i życie człowieka w „ręce" maszynowe. Gorąco dyskutowane obecnie przykłady dotyczą bezpieczeństwa autonomicznych samochodów osobowych, zagadnień wyboru scenariuszy postępowania w przypadku nieuniknionej kolizji i odpowiedzialności prawnej. Dotyczyć to będzie także autonomicznych systemów funkcjonalnych, administracyjnych, produkcyjnych bazujących na IoT, i korzystających z pracy elektronicznych osób. Obszar działań niemoralnych w świecie wirtualnym IoT jest ogromny. Wystarczy uzysk produkcyjny ustawić na maksimum za wszelką cenę. Wystarczy, że 'pozwoli' się osobom elektronicznym zawiązać konspirację. Wystarczy, że wirtualna rzeczywistość IoT obszaru biznesowego firma – klient jest spolaryzowana. Pojawia się konieczność utworzenia prawa dla osób elektronicznych, które na razie dla nas na tym etapie rozwoju są elementem IoT, ale kiedyś będzie to musiało być zmienione. Osoby elektroniczne będą wykonywały konkretną płatną w świecie realnym pracę całkowicie zamiast lub częściowo za danego człowieka. Działanie takiej osoby musi zostać opłacone i państwo powinno pobrać od tej pracy stosowny podatek. Osoba taka powinna być ubezpieczona. Utworzenie prawa dla świata inteligencji infrastrukturalnej, IoT, osób elektronicznych, działalności usługowej i gospodarczej w świecie wirtualnym jest wcześniej czy później konieczna. We Francji ciągle rozważa się wprowadzenie takiego prawa już wkrótce, choć pierwsza propozycja została niedawno odrzucona. Szerokim oddźwiękiem na świecie odbiła się niedawna publiczna wypowiedź Billa Gatesa dotycząca opodatkowania działalności robotów zabierających pracę ludziom.

IoT będzie prędzej czy później ingerował w otoczenie humanistyczne człowieka, jak sfery wychowania, edukacji i kształcenia, mediów informacyjnych, kultury i sztuki, publikacji oraz nauki. W zaawansowanym społeczeństwie opartym na wiedzy, a więc otoczonym inteligentnym środowiskiem infrastrukturalnym IoT, prędzej czy później trzeba będzie zadać sobie pytanie czy szkoła w obecnej postaci spełnia swoje zadanie? Postawienie takiej kwestii dzisiaj znowu wydaje się absurdalne i obrazoburcze. Jesteśmy tak przywiązani do obecnej szkoły? Nie utrzymamy jej w takiej postaci. Czy IoT rozwinie dostatecznie moduły wychowawcze i edukacyjne (Etter 2017)? Przecież rozwinie moduły wspomagania i kontaktu z przedsiębiorcą, managerem, klientem, lekarzem, pacjentem, kierowcą, pilotem, człowiekiem. To nie rozwinie modułów szkolnych? Obecnie rozumiany IoT jako infrastruktura maszynowa, będzie coraz bardziej integrowany z bezpośrednim otoczeniem człowieka, także jego wychowaniem i edukacją, aż dojdzie w pewnym sensie do zaniku granicy, 'rozmowa między maszynami', a pośrednia czy bezpośrednia obsługa człowieka. Chyba że będziemy tej granicy specjalnie strzegli jak źrenicy oka, przy pomocy wirtualnej broni i wirtualnych drutów kolczastych. Czy to znaczy, że szkoła zmieni się kiedyś w wielką instrukcję obsługi rzeczywistości cyfrowej? Czy to znaczy, że szkoła będzie musiała się zmienić z uczenia nas lokalnego lub szerszego patriotyzmu, geografii, historii i języków, matematyki i fizyki, biologii i astronomii w uczenie nas człowieczeństwa – zrozumienia, solidarności, uczciwości, poświęcenia, przyjaźni, tolerancji, przydatności, funkcjonalności, oddania, poświęcenia, miłości, caritas, itp. A jeśli w pewnym momencie, w odległej przyszłości, IoT będzie wyposażony także i w te cechy, w odniesieniu do kontaktów z człowiekiem? W każdym razie dzisiaj w konserwatywnym świecie akademickim rozważa się poważanie nad zmianami klasycznego cyklu nauczania, obejmującego także prowadzone statycznie wykłady przy tablicy. Treść tych wykładów na ogół znajduje się w znacznie rozszerzonej i pogłębionej formie w sieci. Pokolenie cyfrowe na takie wykłady przestaje chodzić. Młodsi i aktywni wykładowcy i nauczyciele z lekcji i wykładów robią atrakcyjne pokazy multimedialne, i to jeszcze jest kupowane. Nie ma wątpliwości, że szkoła będzie musiała ulec zmianie. Wydaje się, że obecnie najbardziej i najszybciej w obszarze edukacji zmieni się pod wpływem IoT kształcenie zawodowe. Ten bardzo ważny sektor kształcenia, skasowany niepotrzebnie w Polsce jakiś czas temu, teraz się systematycznie i dynamicznie odbudowuje na różnych platformach, klasycznej ale także internetowej, kształcenia na odległość, MOOC – *Massive Open Online Course*, i edukacyjnych suługach IoT. Kształcenie zawodowe w przestrzeni IoT stanie się podstawową platformą specjalistycznego kształcenia ustawicznego. Przewiduje się, że IoT może wręcz dokonać powszechnego przełomu w kształceniu zawodowym. Znakomite materiały, łatwość dostępu, atrakcyjne metody treningu zawodowego w przestrzeni wirtualnej IoT, sprzężenie zwrotne, zastosowania technologii chat-botów – inteligentnych botów konwersujących, spowodują odwrócenie kolejności kształcenia wg. zasady 'najpierw zawód potem uczelnia'. Tak wydaje się powinno być, jeśli chcemy aby uniwersytet pozostał wolnym uniwersytetem, a nie szkołą zawodową. Kultura, sztuka, nauka ulegają wpływom cyfryzacji. Publikacje naukowe, literatura popularna i piękna nie mają nakładu a są drukowane, jeśli w ogóle, to tylko na żądanie. Druk klasyczny zastępuje cyfrowy papier uzupełniany multimediami, lub pełne rozwiązania audio i video na urządzania przenośne. Telewizja, kino, teatr, archiwa sztuki cyfrowej będą się przenikać, tworząc nowe media, uzupełniane dodatkowymi funkcjonalnościami artystycznymi i informacyjnymi, archiwizacyjnymi i opcjonalnymi pozwalającymi na wirtualne zmiany przebiegu zdarzeń. Tego typu zjawiska cyfrowej i informacyjnej transformacji humanistycznego otoczenia człowieka są przedmiotem wnikliwych badań psychologów, kulturoznawców, socjologów kultury. Przykładem globalizacji i IoT-yzacji publikacji naukowych jest firma Clarivate Analytics, zatrudniająca ponad 4000 pracowników, i łącznie z wydawnictwem Elsevier prawie całkowicie globalnie monopolizująca i rozwijająca ten sektor, zarówno pod względem finansowym, e-analityki, ale także prestiżowym.

Administracja, usługi, przedsiębiorczość to obszary ściśle związane z człowiekiem. Rozwój sieci globalnej, ICT i IoT zmienia istotnie te obszary. Jaki sens ma posiadanie przy sobie portfela, banknotów, blankietu prawa jazdy, lojalnościowej karty klienta, klubowych kart wstępu, uprawnień dostępu, uprawnień do zniżek i innych przywilejów związanych z wiekiem, kart sportowych, kart bibliotecznych, uprawnień zawodowych, dowodu osobistego, paszportu, dokumentacji zdrowia, karty debetowej i kredytowej, świadectwa maturalnego, dyplomów uczelni, świadectw znajomości języków obcych, książeczek rejestracyjnych pojazdów z aktualnym badaniem technicznym, w przypadku dostatecznie rozbudowanej administracyjnej i usługowej infrastruktury sieciowej IoT. Prace są prowadzone praktycznie wszędzie nad systemami e-administracji, e-samorządu, e-zdrowia, e-edukacji, e-managementu, e-finansów, e-podatków, e-biznesu, e-kultury i innymi podobnymi o zasięgu lokalnym, firmowym, terytorialnym i przede wszystkim ogólnokrajowym. Trudno sobie wyobrazić działalność biznesową, gospodarczą, zarządzanie przemysłem w niedalekiej przyszłości bez coraz intensywniejszego wykorzystania sprzężonych technologii ICT i IoT. Trudno sobie wyobrazić systemy administracyjne nie wspomagające działalności gospodarczej. W niektórych krajach europejskich, podobnie jak w Polsce, fragmenty takich systemów są wprowadzane, testowane lub już działają. Stosunek do wirtualizacji administracji i usług zmienia się. Wymaga to jednak czasu i 'dojrzenia' decydentów. Stosunkowo niedawno temu w Polsce była głośna sprawa ukarania prawnego grupy osób które odważnie podjęły się testowego wprowadzenia regionalnych elektronicznych kart zdrowia na Śląsku, i co gorsza taki system na pewien okres wprowadziły. Kolejne zawiadomienia o rozszerzaniu zasięgu takich usług IoT budzą czasami mieszane uczucia, związane zarówno z brakiem dzisiaj przygotowania infrastrukturalnego, niegotowością użytkowników, barierami psychicznymi, ale także często przedwczesnością czy niedoskonałością projektu. Można tutaj podać przykłady zamieszania w kilku miejscach na świecie związane z systemami e-głosowania, lub klasycznego głosowania wspomaganego internetowo i poważnych oskarżeń o nieprawidłowości. Mimo to rozbudowane systemy e-głosowania są coraz powszechniejsze. W obszarach samorządowych, społecznościowych i pozarządowych systemy e-głosowania połączone np. z usługami stowarzyszeniowymi, członkowskimi wyparły klasyczne głosowanie, opiniowanie i usługi prawie całkowicie. Także wiele innych dostępowych usług IoT włączanych jest coraz powszechniej w portale rządowe, samorządowe i społecznościowe. To między innymi IoT będzie odpowiedzialny za budowę świata bez klasycznej autentykacji, bez haseł, które stały się dzisiaj utrapieniem wraz ze znacznym i ciągłym zwiększaniem się liczby kanałów dostępu do usług sieciowych i IoT. Zgrabna myśl „a world without passwords" stała się nośnym mottem działania niektórych społecznościowych grup rozwijających technologie IoT. Póki co, w okresie przejściowym który będzie trwał prawdopodobnie jeszcze dość długo, niektórzy z nas noszą sprzęgnięty ze smartfonem e-portfel – np. Woolet 2.0, a także wprowadzamy obligatoryjnie, prawnie, antropometryczny dowód osobisty i paszport.

W innym przypadku dane antropometryczne każdego z nas musiałyby być dobrze zorganizowane, zabezpieczone i dostępne mimo wszystko wielopoziomowo w IoT. Nikt zapewne nie chciałby utracić swojej identyczności, a miejmy nadzieję że tylko nieliczni chcieliby swoją identyczność zmienić lub z kimś się zamienić. Wydaje się, że w przyszłości jednym z głównych, jeśli nie jedynym, kanałem dostępu człowieka do spersonalizowanych usług IoT będzie biometria. Nad czym pracuje nauka i przemysł w tym zakresie. Bezpieczeństwo i jeszcze raz bezpieczeństwo, a oprócz tego testowanie nowych obszarów aplikacji, np. próby znacznego rozszerzenia aplikacji e-zdrowie, standaryzacja, rozpowszechnianie szeroko międzynarodowo negocjowanych w grupach roboczych systemów open source, zasięg, skalowanie, koszt, stopień skomplikowania, podatność rozwojowa, odporność na pracę w trudnych warunkach, adaptacyjność i akceptowalność indywidualna i społeczna, itp. (Zarko 2016), (Zhang 2015). Ze względna na zaangażowanie w projekty rozwojowe IoT w obszarze administracji i usług znacznych środków publicznych i prywatnych, kategoria adaptacyjności i akceptowalności staje się jedną z najważniejszych. Odpowiednia technologia IoT istnieje i może być niemal natychmiast szeroko zastosowana, wymaga tylko adaptacji, powielenia i sporych inwestycji, ale czy zostanie zaakceptowana? Niestety nowe technologie znacznie wyprzedzające rozumienie i potrzeby rynku muszą być poprzedzone kosztownym i ryzykownym 'uczeniem rynku'. Bardzo rzadko odnosi się w zakresie implementacji nowych technologii na rynku sukces biznesowy przez zaskoczenie. Niewiele firm innowacyjnych, spośród których duża część to małe przedsiębiorstwa skupione wokół jednego lub kilku dobrych pomysłów, stać na dużą i kosztowną akcję uczenia rynku. W przypadku globalnych technologii korzystnych dla społeczeństwa rolę nauczyciela i wprowadzającego pełni państwo, wielkie korporacje i największe organizacje społecznościowe. Tak dzieje się np. z ogólnoeuropejską inicjatywą Photonics21 której rolą, we współpracy z programami europejskimi FP7, H2020 i następnie FP8 jest znaczne upowszechnienie implementacji fotoniki w gospodarce IoT, rozwoju ochrony zdrowia, energetyki i nowej generacji oświetlenia, Internetu przyszłości, oraz sprzętu użytkowego. W skali europejskiej jest kilka takich aktywnych obecnie inicjatyw, obejmujących swoim działaniem technologie IoT, z których główną wydaje się e-zdrowie. Ile czasu trwa przekonanie masowego konsumenta do wymiany źródeł światła z żarówek na DEL? Różnica ceny jest znaczna, a efektwność energetyczna nie do końca rozumiana!

Kolejnymi obszarami wokół człowieka w którym IoT wypiera technologie klasyczne są relacje publiczne PR, inaczej imagistyka społeczna, marketing i branding, a ogólniej e-biznes. Jeszcze cały czas takie technologie odgrywają znaczną rolę jak np. reklama miejska, TV i optymalizacja przeszukiwarek internetowych SEO – search engine optimization w budowaniu opinii i pozycji, poszukiwaniu odbiorców docelowych, ale IoT zaczyna i będzie przeważać. Techniki SEO mają na celu poprawianie pozycjonowania firmy czy produktu i były związane z szeregiem metod na pograniczu uczciwości. Google, na ogół dość skutecznie choć z opóźnieniem, reaguje na coraz bardziej wyrafinowane programistyczne techniki 'pompowania' pozycji, nakładając na nadużywające linki i terminy googlowy 'Czarny Kapelusz'. Obszar nieuczciwości jest znaczny i obejmuje np. takie techniki jak optymalizowane „fakenewsy", potężne serwery telefoniczne składające się z wielu tysięcy linii generujące klikalność i „lajki", i inne. Obecnie SEO w formie znacznie bardziej zaawansowanej rozwija się w kierunku marketingu zawartości, marketingu socjalnych środków przekazu i optymalizacji pod smartfony i tablety, a mimo to wydaje się ustępować miejsca mobilnym technikom IoT jak Alexa, AppStore, Dash Button, i inne. Specjaliści od e-handlu mówią wprost, że nadchodzi złota era PR, marketingu i brandingu wraz z rozwojem i coraz szerszym zastosowaniem narzędzi IoT. Żartobliwym odzwierciedleniem tej tendencji wzrostu rynku marketingowego IoT jest zawołanie które pojawiło się niedawno w prasie specjalistycznej 'marry a marketer'. Nowoczesny marketing jest interdyscyplinarny, bazuje na wielu czynnikach jak: tworzeniu modeli psychiki konsumentów i baz danych motywów zachowań, wspomaganej przez IoT analizie wielkich zbiorów danych przy podejmowaniu dobrych decyzji, badaniu relacji społecznych pomagających w znalezieniu metod promocji marki przy pomocy opowiedzenia o niej wyjątkowej i zajmującej historii, wyborze 'wyrafinowanie naturalnych' technik działania w mediach społecznych utrzymujących markę na szczycie list aktualnych i modnych kanałów komunikacyjnych i angażujących bezpośrednio konsumentów, oraz opracowaniu artystycznym i sposobie narracji inaczej storytellingu najlepiej doprowadzającym konsumenta do łez. Celem tego skomplikowanego procesu jest oczywiście spowodowanie kliknięcia przez konsumenta w odpowiedni guzik wirtualnego koszyka zakupowego, lub w wersji audio wypowiedzenie nazwy towaru z jego atrybutami, a w wersji bardziej skomplikowanej podpisanie umowy o dostawie towaru czy usługi. Jedną z czołowych firm pracujących w tym obszarze ICT i IoT, e-konsumentów, e-marketingu, e-biznesu, ale także e-wyborów jest CA – Cambridge Analytica. CA wspomagała informatycznie ostatnie wybory prezydenckie w USA.

Penetracja IoT w obszar e-biznesu jest znacznie głębsza i szersza niż dyskutowano powyżej dla marketingu. IoT zaczyna kompletnie przeorganizowywać ustabilizowane od jakiegoś czasu operacyjne systemy CRM bazujące w wielu przypadkach na mozolnej pracy ludzkiej, szczególnie w takich firmach które widzą, rozumieją i szybko akceptują nieuchronne kierunki rozwojowe. W każdej organizacji największym zagrożeniem dla innowacji jest wewnętrzna polityka i kultura organizacyjna, która nie akceptuje porażki, pomysłów z zewnątrz, i przez to nie potrafi się szybko zmienić. A tutaj mamy IoT który jest potężnym narzędziem dostarczającym danych, analitycznym, marketingowym, sprzedażowym i wsparcia technicznego. IoT korzystając z narzędzi rozwojowych rzeczywistości rozszerzonej, także z technologii gier komputerowych, daje możliwość budowy nowej efektywnej przestrzeni kontaktów biznesowych z rynkiem, klientem, itp. CRM-IoT wyposażony w adekwatną inteligencję biznesową, tworzy wirtualne modele i wielowymiarowo segmentuje klientów, używa interfejsów deskryptywnych audio i behawioralnych do tworzenia nowych funkcjonalności, a przede wszystkim tworzy nową wartość dla klienta. W prostym przypadku może to być np. natychmiastowe przygotowanie skomplikowanego, ale optymalizowanego do danej sytuacji arkusza kalkulacyjnego, jedynie w oparciu o jej opis werbalny. Dalej może być to szybka, wsparta rzetelną analizą danych, atrakcyjna oferta dla klienta. W innym przypadku może to być generacja nowego wskaźnika ewaluacyjnego wykorzystującego inne parametry, złożona przekrojowa analiza statystyczna, a także wielowariantowe obliczenia symulacyjne i estymacyjne dla okresów przyszłych. Rozwój idzie w kierunku zatrudnienia analityki i wielowarstwowe podejście do zagadnienia uwzględniające psychologię, socjologię, kulturę, nawet sztukę wizualną, multimedia, itp. Warunkiem powodzenia jest ciągły dopływ nowych standaryzowanych danych np. z brzegowych obszarów IoT. Biznesowy rynek IoT rozwija się dynamicznie adresując wzrastające zapotrzebowanie (Jamthe 2015), (Kranz 2016). Kluczowe firmy rynku ICT oferują komercyjne platformy IoT. Na platformie IoT firmy budują swój ekosystemem IoT. Platforma IoT jest mostkiem pomiędzy urządzeniami IoT oraz siecią danych. Oferowane obecnie większe platformy to np.: Amazon Web Services, Nokia IoT Grid, Microsoft Azure, ThingWorx IoT Platform, IBM's Watson, Cisco IoT Cloud Connect, Cisco ICN information centric networking, Salesforce IoT Cloud, Oracle Integrated Cloud, GE Predix, EMnify IoT&M2M, ResIoT LoRaWAN, Deutsche Telecom Cloud of Things, i inne. W zasadzie, obecnie większość dużych firm wysoko technologicznych rozwija i stosuje platformy IoT. Niektóre z tych platform są stosowane szerzej, np. do rozwoju technologii 5G i bardzo interesujących dla dalszego rozwoju IoT sieci ultra niskoenergetycznych LPWA – low power wide area.

Potencjał zastosowania IoT w systemie e-zdrowie obejmuje między innymi takie zagadnienia jak bezpośrednia i pośrednia ochrona zdrowia, zdrowotna prewencja społeczna, e-epidemiologia, ogólne statystyki zdrowia społecznego, pacjent rzeczywisty i wirtualny, indywidalna karta zdrowia, firmowe badania okresowe, monitoring i zdalna opieka nad pacjentem, system wspomagania osób niepełnosprawnych i zagrożeniem zdrowotnym, medycyna sportowa, ale także ubezpieczenia zdrowotne, i ogólnie dobrostan człowieka (Bhatt 2017). U nas w kraju środowisko medyczne jest zaskakiwane różnymi oświadczeniami administracji i samorządu zawodowego na temat szerokiej wirtualizacji usług medycznych i całego otoczenia medycyny. Wyprowadzane mają być takie systemy, korzystające szeroko z zasobów IoT, jak np. e-lekarz, e-gabinet, e-przychodnia, e-szpital, e-sanatorium, wymagające wyposażenia wszystkich gabinetów, przychodni, szpitali i innych miejsc usług związanych ze zdrowiem w standaryzowane punkty dostępu i standaryzowane metody wprowadzania, łączenia, i eksportu danych. Opór środowiska lekarskiego budzi fakt obciążenia lekarza dość pracochłonnymi, na obecnym etapie rozwoju takich aplikacji, procedurami pracy z systemem komputerowym. Dostępne i używane systemy są ciągle zbyt słabo zautomatyzowane, zbyt heterogeniczne i mało przyjazne dla użytkownika. Często używa się w nich jeszcze własnościowych formatów plików bazodanowych i graficznych, co w przyszłości jest nie do przyjęcia. Cały czas używana jest w wielu systemach medycznych płyta CD jako historyczny nośnik informacji. Ze względu na ustawowe ograniczenia dostępu

do informacji medycznych właściciele systemów lokalnych stosują własne zabezpieczania, takie na jakie ich stać lub takie jakie potrafią skonfigurować. Nie ma to nic wspólnego ze standaryzacją i kompatybilnością międzysystemową. Rozwój własnych systemów IoT obsługi e-zdrowia jest bardzo kosztowny i wydaje się bardziej ryzykowny ze względu na bardzo eksponowaną pozycję służby zdrowia w społeczeństwie. Jednak mimo to można podać liczne przykłady opracowań IoT dla medycyny i do zastosowań paramedycznych związanych ze zdrowiem. Usługi medyczne są powiązane z ZUSem, ubezpieczeniami emerytalnymi i ubezpieczeniami zdrowotnymi, a więc finalnie w skali krajowej obszar ten jest łączony z dużymi finansami. ZUS jest inicjatorem pełnej elektronizacji swoich usług, poprzez stosowną dedykowaną sieć e-ZUS będącą w przyszłości częścią systemów e-zdrowie i e-pracownik. Do sprawnego funkcjonowania takiej sieci, czyli kontroli nad usługami, finansami, zdrowotnością, potrzebne są dane. Dane zbierane od lekarzy, od pacjentów, dane medyczne, wyniki badań laboratoryjnych i obrazowych, tworzą coraz bardziej uporządkowane zbiory służące do analityki.

Stan zdrowia klienta jest przedmiotem zainteresowania firm ubezpieczeniowych. Klient kosztuje ubezpieczyciela tym mniej im jest zdrowszy. W interesie ubezpieczyciela jest aby klient był zdrowy. Oznacza to że ubezpieczyciel jest zainteresowany danymi dotyczącymi stylu życia klienta, kosztów jego utrzymania codziennego, podatności na zachowania ryzykowne, np. czy dba o zdrowie, jak często przeprowadza badania okresowe, czy prawidłowo dba o kondycję i uzębienie, w jakim stylu prowadzi samochód, zanim nie wprowadzą prawa samochodów autonomicznych. Na pierwszy rzut oka wydaje się to śmieszne. Tak jednak nie jest. Anegdota o elektrycznej zinternetyzowanej szczoteczce do zębów monitorującej czas i intensywność higieny jamy ustnej i dostarczającej te dane poprzez złącze USB doładowania do domowego archiwum zdrowia, a potem ewentualnie do ubezpieczyciela nie jest potencjalnie zupełnie nieprawdziwa. A przecież poniżej piszemy wymieniając także szczoteczkę jako jeden z elementów Internetu Rzeczy Niepotrzebnych. Tak to jest dzisiaj, IoT jest pełen paradoksów wieku dziecięcego. A to już nie anegdota tylko fakt. Firma SI produkująca masażer We-Vibe Tango została oskarżona, być może niesłusznie, o to że przyrząd ładowany przez USB dostarcza dane dotyczące czasu i intensywności masażu oraz dokonuje lokalnych pomiarów temperatury. Telewizory Samsunga serii smart były podejrzane o podsłuchiwanie użytkowników poprzez aplikację sterowania głosem. Krajowym przykładem znakomitego nowatorskiego urządzenia IoT jest monitor piersi zaprojektowany, opatentowany i produkowany od niedawna przez firmę Braster. Kubek pomiarowy nakładany na pierś tworzy w matrycy ciekłokrystalicznej obraz rozkładu ciepłoty na powierzchni piersi. Obraz poprzez złącze USB i komputer domowy oraz konto abonenckie pacjentki podlega akwizycji i przetwarzaniu w firmie. Obrazy zapisywane systematycznie podlegają porównaniom między sobą i z wzorcowymi obrazami odniesienia standaryzowanymi względem różnic anatomicznych każdej osoby. Na podstawie zbioru danych system ekspercki podejmuje decyzję o ewentualnym ostrzeżeniu pacjentki. Życzymy firmie sukcesu biznesowego z tym świetnym pomysłem, choć na razie chyba takiego sukcesu nie ma, co jest spowodowane barierami psychologicznymi. Zestaw Braster do monitoringu piersi jest dostępny w niektórych aptekach lub w Cefarmie.

Ze zdrowiem związana jest także problematyka uzależnienia cyfrowego. Funkcjonuje takie pojęcie jak detoksykacja cyfrowa. Związane jest ono w pewien sposób z psychologią, medycyną, a szczególnie z medycyną uzależnień. Dzisiaj nadmierne używanie systemu cyfrowego w wielu jego odmianach nazywamy już nałogiem cyfrowym, uzależnieniem od Internetu, ale także od urządzeń IoT. Nałóg cyfrowy jest badany jako nowe zjawisko. Mówi się o metodach detoksykacji cyfrowej. To kolejny związek IoT z człowiekiem. Nie najlepszy związek z którym trzeba sobie będzie poradzić. IoT staje się coraz bardziej interaktywny z człowiekiem, i potencjalne niebezpieczeństwo tkwi właśnie bardziej w tym niż w pasywnym odbiorze. Przerażające doniesienia prasowe z zagranicy o wpływie interaktywnej gry internetowej Niebieski Wieloryb na młodzież przekonują, że to jest realne zagrożenie. Jednocześnie interaktywne gry stają się obecnie elementem budowy także biznesowej, gospodarczej, nawet medycznej warstwy IoT, a nie tylko rozrywkowej. W pewnym momencie mogą stać się także ważnym elementem gry politycznej.

Nad czym pracuje nauka w obszarze IoT i zdrowie. Główne kierunki prac wymieniane skrótowo i arbitralnie to: masowy rozwój pomocy dla osób niepełnosprawnych ruchowo, słuchowo i niewidomych, rozwój aparatury medycznej, źródeł danych o ciele człowieka w tym jego osobistej struktury DNA, aparatury obrazującej, minimalno-inwazyjnych metod endoskopowych, automatyzowanych analitycznych metod laboratoryjnych, połykane mikrosystemy funkcjonalne (np. Origami MIT), robotyka pielęgniarska, medyczny druk 3D, operacyjnej mikrorobotyki endoskopowej, nanorobotyki endoskopowej oddziaływującej z systemem immunologicznym człowieka, metod diagnostycznych wspomaganych ICT, skórą bioniczną kompatybilną ze skórą człowieka i mierzącą parametry fizjologiczne, a wkrótce operacyjną technologią rzeczywistości rozszerzonej. Nie sposób tych zagadnień tutaj szerzej omówić. Wspomnijmy jedynie o potencjalnej roli wielkich zasobów danych przydatnych dla diagnostyki medycznej. Dane te obejmują zarówno takie które pochodzą ze źródeł medycznych dotyczących indywidualnego człowieka, ale również epidemiologicznych, statystycznych, antropometrycznych, laboratoryjnych biochemicznych, a także ze źródeł IoT. Badania mechanizmów nowotworowych u człowieka w oparciu o analizę i tworzenie wiedzy z wielkich zbiorów danych metodami IoT prowadzone są w kilku ośrodkach na świecie, między innym w Uniwersytecie Cornell. Projekt 'Nowotwór i Big Data' zorganizowany jest wokół wydawałoby się całkiem 'kosmicznej' tezy, że jeśli posiadalibyśmy dokładne dane DNA setek milionów ludzi i dane laboratoryjne DNA mutujących nowotworów zbierane automatycznie metodami robotycznymi IoT, to możliwe byłoby poznanie mechanizmów ich rozwoju i w konsekwencji skuteczne zwalczenie. Dlaczego rozwiązaniem jest zastosowanie technologii Big Data i globalnej, standaryzowanej automatyzacji metodami IoT? Pojedynczy nowotwór posiada 100 miliardów komórek. Każda z nich mutuje szybko, adaptacyjnie i indywidualnie. Zrozumienie mutacji, utworzenie ich modeli, wymaga robienia milionów 'fotografii' DNA w czasie tych zmian i budowy bazy danych oraz kategoryzacja takich zmian. Nie ma wątpliwości, że zebranie danych DNA miliarda ludzi jest problemem ekonomicznym, ale głównie politycznym, przekraczającym obecnie możliwości ludzkości na tym etapie rozwoju. Czy kiedyś takie bariery przekroczymy? Czy trzeba je przekraczać? Czy nie wymyślimy innych metod? Niektóre zgadanienia rozwiązuje się metodami obliczeniowymi Monte Carlo, czyli pełnej analizy bez dróg na skróty. To jest prawdopodobnie także taki przypadek. Do rozwiązania tego typu zadań, których jest jeszcze nie rozwiązanych dużo, potrzebe są narzędzia: szybkie komputery, inteligencja obliczeniowa, robotyka i IoT.

Kolejna warstwa oddziaływania IoT z człowiekiem to transport osobowy i związany bezpośrednio z człowiekiem, np. przekazywanie przesyłek między ludźmi, z instytucji, sklepów. Ogólnie dziedzina IoT -yzowanego transportu jest oczywiście szersza. Obejmuje transport masowy, statkami, kontenerami, pociągami, ciężarówkami, samolotami, transport detaliczny, dronami, w przemyśle między systemami produkcyjnymi, i wiele innych. Niektóre sektory przemysłu stosują technikę dostarczania elementów produkcyjnych dokładnie na czas, co wymaga zastosowania precyzyjnej logistyki transportu. Dzisiaj jednak słowem kluczem, odmienianym przez wszystkie przypadki z dodatkiem wielu przymiotników, jest samochód osobowy bez kierowcy. Wymieńmy w skrócie niektóre zagadnienia z tym związane, oprócz kolejnych bardziej zawansowanych generacji oprogramowania takiego samochodu i systematycznego wzrostu inteligencji operacyjnej działającej w czasie rzeczywistym. Jedną z głównych warstw systemu autonomiczny samochód – inteligentna droga jest transmisja danych i przetwarzanie tych danych na informacje kursowe dla samochodu, bezpieczeństwo, poprawę komfortu jazdy, informację dla pasażerów, itp. Transmisja danych może obejmować komunikację między samochodami, tworzenie sieci ad hoc aut poruszających się obok siebie, komunikację auta z 'inteligentną' drogą, znakami drogowymi poziomymi i pionowymi, z otoczeniem drogi, systemami IoT specjalizowanymi do obsługi, nadzoru i optymalizacji ruchu drogowego, elementami systemu pomocy drogowej i bezpieczeństwa, czy z adekwatną infrastrukturą w pobliżu. Jeśli wszystkie samochody będą autonomiczne to być może nie będą potrzebne światła drogowe w inteligentnym mieście. Taki system Car-Net wprowadza np. już obecnie VW. Asystent Car-Net mówi także doskonale po polsku. Transport towarów i osób bez kierowcy, rozwijany i organizowany jako element globalnego systemu IoT, będzie jednym z głównych czynników kompletnie zmieniających naszą cywilizację. Mamy dzisiaj nadzieję, że uczyni ją bardziej produktywną i bardziej bezpieczną. W dużych miastach miliony kierowców dojeżdżają codziennie do pracy samochodami co zajmuje często wiele czasu. W czasie podróży człowiek nie jest specjalnie produktywny. Samochód bez kierowcy uruchamia w człowieku zablokowaną wielozadaniowość. IoT nas efektywnie i bezlitośnie eksploatuje mówiąc pesymistycznie i mało delikatnie, lub pomaga nam w pracy mówiąc optymistycznie. Inne warstwy IoT także mogą być ukierunkowane na przeorientowanie zadań i przyzwyczajeń człowieka, tak aby lepiej wykorzystać jego możliwości. Nad czym pracuje

nauka w tym zakresie rozwojowym IoT. Przede wszystkim nad tworzeniem systemów operacyjnych czasu rzeczywistego klasy RTOS do bezpiecznej obsługi pojazdów autonomicznych. Takie specjalizowane systemy, o węższych funkcjonalnościach, optymalizowane do aplikacji, jednak przewidujące zachowanie wszystkich elementów kontrolowanego systemu, były rozwijane już od dłuższego czasu dla przemysłu, lotnictwa, techniki kosmicznej i dla wojska. System operacyjny RTOS odrzutowca wojskowego musi uwzględniać np. sytuację chwilowego ograniczenia funkcjonalności czy nawet utraty przytomności pilota spowodowaną dynamicznym przeciążeniem grawitacyjnym. Znaczne powiększenie zastosowań IoT spowodowało konieczność zupełnego przedefiniowania funkcjonalności systemów operacyjnych czasu rzeczywistego i zwiększenia ich różnorodności. Nauka i przemysł współpracują w zakresie samochodu autonomicznego nad systemowym rozwiązaniami bezpieczeństwa. Na przykład, seria obszernych analiz firmy IBM pod wspólnym tytułem „Auto 2025" przygotowana we współpracy z kilkunastoma tysiącami ankietowanych specjalistów, producentów i użytkowników, dotyczy przyszłości autonomicznego samochodu osobowego, głównie w aspektach 'nowego bezpieczeństwa' związanego z rozwojem technologii IoT oraz rozwojem przemysłu motoryzacyjnego, a także sektorów gospodarczych silnie zależących od samochodu. Coraz częściej firmy motoryzacyjne współpracują z elektronicznymi, ICT i telekomunikacyjnymi nad rozwiązaniami dla osobowych samochodów autonomicznych. Tak jest np. w przypadku Audi i Nvidia, stosujących technologie 'Głębokiego Uczenia' dla samochodowego systemu sztucznej inteligencji.

Transport człowieka dla przyjemności, dla zdrowia, czy także funkcjonalny to także motocykl i rower. Prace nad bezpiecznym rowerem i nieprzewracającym się motocyklem są prowadzone przez kilka firm, np. przez BMW. Projekt motocykla IoT jest rozwijany pod chwytliwą nazwą handlową 'motocykl nie wymagający hełmu'. Motocykl zapewnia zupełnie nowy poziom bezpieczeństwa. Jest zupełnie nieprzewracany, kontroluje rodzaj nawierzchni, poziom bezpieczeństwa, wspomaga początkującego motocyklistę, daje inne możliwości motocykliście zaawansowanemu, itp. Cały krytyczny układ kontroli motocyklu jest połączony z zaawansowanym wizjerem, który ma postać lekkich plastikowych przezroczystych okularów dla kierowcy. W sensie swobody jazdy i poczucia wiatru we włosach motocykl IoT daje poczucie powrotu do początku motocyklingu, gdy nie były wymagane żadne hełmy. W sensie prawnym i technicznym można liczyć się z dopuszczeniem w przyszłości takiej maszyny do ruchu bez używania hełmu przez kierowcę. Z branży rowerowej, konieczne jest wymienienie tutaj znakomitego systemu warszawskiego roweru publicznego IoT Veturilo. Veturilo wprowadziło ostatnio rowery dla dzieci Veturilko, i w liczebności dostępnych pojazdów zbliża się do 5000. Zapowiada także wprowadzenie rowerów elektrycznych. Rowery są wypożyczane głównie przez aplikację mobilną. Rower IoT wyposażany będzie niedługo we wspomagający miniaturowy silnik elektryczny używany w miarę potrzeby, systemy pomiarowo-kontrolne i diagnostyczne, ograniczniki prędkości, analizę nawierzchni, inteligentne oświetlenie, itp. W drugiej połowie 2017 r. Warszawa planuje uruchomienie wypożyczalni miejskich samochodów IoT w formule współdzielenia samochodu, podobnej do funkcjonującego od niedawna rozwiązania w Berlinie. Początkowo będzie to ok. 500 pojazdów IoT. Symulacje pokazują, że jeden samochód współdzielony przez wielu użytkowników w gęstej przestrzeni miejskiej może zastąpić ok. 10 aut prywatnych. W Warszawie na 1000 mieszkańców przypada ok. 640 aut prywatnych. Powodzenie akcji będzie zapewne zależeć od ceny wypożyczenia.

IoT zmienia masowy i indywidualny transport towarów. Nie ma uzasadnienia już dzisiaj aby transport morski obsługiwany na stałych liniach przez wielkie tankowce, masowce i inne duże statki towarowe posiadał załogę ludzką, spędzającą dość bezproduktywnie miesiące czasu na pokładzie. Nawigacja satelitarna, znajomość dróg morskich, systemy bezpieczeństwa np. INMARSAT, niezawodność napędów i sterowania są tak zaawansowane, że od przemierzających oceany dużych statków „widm" dzieli nas dosłownie chwila. Trudniejszy do zautomatyzowania jest transport lądowy, ale i tu ciężarówki kontenerowe są wyposażane w sprzęt prowadzący wcześniej czy później do częściowej i następnie pełnej autonomii. Daimler prowadził już testy autostradowe autonomicznej ciężarówki Future Truck FT2025. Ciężarówka jest jeszcze nadzorowana przez kierowcę ze względów formalno-prawnych, związanych z legalizacją transportu autonomicznego. Być może opłacalna będzie budowa zupełnie odrębnych dróg dla takiego transportu i nie mieszania go z transportem osobowym. Autonomizacja dotyczy także masowego transportu kolejowego i lotniczego. Prowadzone są prace projektowe nad dużymi oszczędnymi dronami transportowymi o nośności ponad 100 ton z napędem odrzutowym. Drony takie według obecnych projektów będą poruszały się z prędkościami ok. dwukrotnie mniejszymi od samolotów pasażerskich i na mniejszych wysokościach, zużywając znacznie mniej paliwa. Internetyzacja infrastruktury transportowej i innej będzie zapewne przebiegała różnymi drogami, inaczej i raczej niezależnie dla systemów małych, bezpośrednio funkcjonalnych, blisko otaczających człowieka, dużych systemów nieprodukcyjnych usługowych, a przemysłowych systemów produkcyjnych. Różnego rodzaju drony opracowywane są dla celów bezpieczeństwa i obronności, np. Salty Dog 502.

Inteligentny dom, dom IoT, jest obecnie już najbardziej skomercjalizowaną częścią rozwijającego się obszaru inteligentnej infrastruktury oddziałującej pośrednio i bezpośrednio z człowiekiem. Na rynku komercyjnym urządzeń IoT, za granicą i w kraju, dostępnych jest wiele rozwiązań sprzętowych i programistycznych obsługujących poszczególne podsystemy i zapewniające odnowione, rozszerzone i nowe funkcjonalności. Ewolucja w kierunku domu IoT postępuje na ogół poprzez doposażanie istniejących budynków i mieszkań w nowe rozwiązania inteligentne. Nowa obecnie budowana infrastruktura mieszkaniowa jest w niektórych przypadkach wyposażana w rozwiązania ułatwiające instalacje urządzeń IoT, np. centralne serwerownie, repozytoria danych, panele użytkownika, sieć Wi-Fi, światłowody infrastrukturalne, wielopoziomową kontrolę dostępu, a także inteligentną łazienkę, stałe urządzenia AGD klasy IoT, inteligentne okna, ogrzewanie i klimatyzacja, i wiele innych. Nauka w tym obszarze pracuje np. nad rozszerzeniem rodzajów czujników możliwych do zastosowania w inteligentnym domu oraz nad integracją systemów IoT z infrastrukturą budowlaną. Na przykład inteligentne okna, co wymaga zastosowania aktywnych szkieł, reagują na wilgotność, oświetlenie i temperaturę na zewnątrz i wewnątrz pomieszczania, odpowiednio zmieniając swoją przepuszczalność termiczną i optyczną. W Internecie można znaleźć aplikacje sprawdzające IQ mieszkania i budynku na podstawie testowania sieci urządzeń inteligentnych i sposobu ich reakcji. Większość z rozwiązań kontroli domu IoT jest dostępnych także przez smartfon. Zagadnienie inteligentnego domu jest przedmiotem rozważań w innym rozdziale niniejszej monografii stąd ograniczymy się dalej do wymienienia niektórych z licznych dostępnych na rynku firmowych, sprzętowych i aplikacyjnych rozwiązań komercyjnych, grupując je funkcjonalnie. Wymienione poniżej aplikacje posiadają bardzo różne funkcjonalności. Niektóre ograniczone są do jednej bardziej skomplikowanej czynności, do grupy podobnych, a niektóre są uniwersalne i pokrywają cały obszar swojej specjalności.

Monitorowanie dzieci, i zwierząt domowych: iBaby, Petnet, Petcube, Nanit, Sevenhugs, Lully, Aristotle, Rapid7, MimoBaby, Snoo Smart Crib, Owlet, Withings Home, Kinsa, Pacif-i smart dummy, Garmin Babycam;

Monitorowanie osób starszych i niepełnosprawnych w domu: 22CityLink, IBM, BodyGuardian, BeClose, WT – Wearable Technologies, UnaliWear;

Systemy i urządzenia audio: Hiku, Independa, Innit, Sonos, Musaic, Kitu, SectorQube, Hiku;

Oświetlenie: Lumetric, Plum, Switchmate, Emberlight, Lifx, Philips Hue;

Energia, klimatyzacja, narzędzia techniczne: Ecoisme, Sense, Thinkeco, Racio, Kamarq, Notion, Ecobee, There, Tado, Ecovent, Netatmo, Keen, Vivint,

Ogród: Nexwell, Grove, Niwa, Edyn, Ambrogio L250 Elite, mesur.io;

Roboty domowe: Jibo, Rokid, Robart, Neato, Kuri;

Czystość w domu: Rowenta RR011, iRobot Romba 616, 876, 886 i 966, PowerBot Samsung, Neato Robotics Botvac D, Hoover RBC;

Zdrowie i samopoczucie: Beddit, Hello, Medminder, LinkLabs, AugMedix, Voluntis, NeuroVigil, BL Healthcare, proteus, Pristine;

Kontrolery/sterowniki urządzeń, automatyka domowa i budynkowa, managery: Fibaro, Grenton, Sentri, Fluent, NinjaBlocks, Muzzley, Wigwag, Ivee, Peel, Avi-on, iRule, ExtraLife, Ira, Vbass, eHouse, Bmg SmartLiving, Elektris, FDtech, xComfort, Somfy, Nexwell, Belkin WeMo, NevonProjects, ElProCus;

Bezpieczeństwo i ochrona: Leeo, BeONhome, SimpliSafe, Roost, MyAlarmCenter, Myfox, August, Lockitron, Ring, Canary, Latch, Audio analytic, Coccon, Glue, Edgefinity-Cybra, Eset, panStamp, Cumulocity, Nightingale Security, Indiegogo, Sunflower HAS, Aptonomy;

Platformy integracyjne IoT: Azure, AWS, Zatar, ThingWorx, IBM Watson, Bosch IoT Suite, Plat.One, Everything IoT, Ericsson IoT, 2lemetry IoT, Appcelerator, ParStream, Tekwissen;

Możliwe jest tutaj omówienie zaledwie kilku wybranych przykładów urządzeń funkcjonalnych IoT dla domu i jego otoczenia. Robot koszący, inteligentna kosiarka Ambrogio L250 Elite zapamiętuje roz-

kład ogrodu i znajdujących się przeszkód, uczy się planu całej okolicy działania, nie tylko obszaru trawnika, jest podłączony do chmury a karta SIM i pamięć wewnętrzna powala uruchomić maszynę zdalnie w dowolnej chwili i wybrać stosowny program operacji w tym adaptację do warunków otoczenia, koordynację z system podlewania i z prognozą pogody. Zaawansowane komercyjne systemy bezpieczeństwa dla większych posiadłości stosują autonomiczne drony podrywane w razie konieczności. Dron, lub kilka dronów, posiada garaż z dokowaniem np. na dachu budynku, jest uruchamiany autonomicznie natychmiast w przypadku alarmu i operuje w powietrzu nawet do 30 minut. Funkcjonalność obejmuje nagrywanie sekwencji wideo, dokumentację wydarzeń, oświetlenie terenu w pasmach IR i VIS, wygłaszanie komunikatów ostrzegawczych, okresowe krótkie zaprogramowane przeloty nad monitorowanym terenem, informacje doraźne i zbiorcze dla mieszkańców, alarmy dla służb ochronnych, itp. Kontrolery IoT domowych urządzeń funkcjonalnych i sprzętów domowych powszechnego użytku są coraz częściej produkowane w formie dokładnie kompatybilnej z analogicznymi urządzeniami biernymi poprzednich generacji. Pozwala to na prostą wymianę włączników/wyłączników światła i innych urządzeń jak pralki, regulatorów ogrzewania, zamków, nawilżaczy powietrza, monitoringu dostępu, itp. ze starych na usieciowione. Domowa e-opieka nad osobami starszymi, związana najczęściej z elektroniką ubieralną, obejmuje monitorowanie parametrów życiowych, pozycji, ruchu, przypomnienia przyjmowania leków, alarmy, wspomaganie ruchu, itp. Takie proste i bardziej skomplikowane urządzenia domowe ożywiające rzeczy są właśnie wymienione na wybranych listach powyżej.

IoT ma zamiar pozbawić nas w przyszłości przyjemności chodzenia do sklepów i centrów handlowych. Na razie jednak ten e-handlowy sektor IoT rozwija się dynamicznie. Wzrasta znacznie rola RFID, NFC, BT, i pokrewnych technologii lokalizacji i identyfikacji lokalnej, oraz przesyłania danych. Funkcjonalność systemów RFID i NFC rozszerza się i ta tendencja jest rozwijana zarówno ilościowo jak i jakościowo. Wchodząc do dużego centrum handlowego, czy poruszając się po śródmiejskiej części miasta jesteśmy i tak dokładnie lokalizowani i identyfikowani przez gęstą sieć telefonii mobilnej i innych sieci proksymalnych. W hurtowniach jesteśmy identyfikowani przez karty klienta obowiązkowo logowane do systemu sklepowego przy wejściu i wylogowywane przy wyjściu w wirtualnej kasie. Karty dostępowe RFID do hurtowni i innych miejsc gdzie są wymagane można deponować w komórce. Inteligentny wózek sklepowy wyposażony w skaner RFID wykazuje na wyświetlaczu listę kupowanych towarów i podlicza zapłatę, która uiszczana jest automatycznie podczas wychodzenia ze sklepu, jakby w wirtualnej kasie, której oczywiście nie ma. Lista zakupów z komórki pojawia się na wyświetlaczu w wózku sklepowym, jeśli wybierzemy taką opcję, i informuje nas czego jeszcze nie kupiliśmy. Przy masowym połączeniu wielu produktów poprzez IoT konsumenci dostają nowe możliwości wyboru i podejmowania decyzji. Urządzenia AGD oceniają same zapotrzebowanie na podstawowe produkty, lodówka na świeżą żywność, pralka na proszki do prania, odkurzacz i system czyszczący na środki czystości. Odrębne panele sterowania urządzeń pewnie będą formą przejściową, jak zamawianie produktów prosto z panelu urządzenia. Przykładem takiego rozwiązania jest praktyczny, uniwersalny, obecnie programowalny IoT Amazon Dash Button, jednoprzyciskowy mini terminal do zakupów, łączący skaner i interfejs głosowy z listą zakupów. Rozwiązanie to zebrało wiele kontrowersyjnych opinii w prasie popularnej, ale jego wielką zasługą jest dalsze zwiększanie stopnia zaprzyjaźnienia społeczeństwa nietechnicznego z gadżetami IoT. Coraz większa część życia człowieka będzie związana z IoT, co spowoduje automatyzację obsługi coraz większej części zadań rutynowych, standardowych, powtarzalnych, uwalniając człowieka od tego i dając mu więcej czasu na rodzinę, rozrywkę i odpoczynek, hobby i oczywiście twórczą pracę. Tam gdzie jednak chcemy podjąć decyzję sami, będzie ona ułatwiana przez dostęp do optymalizowanych danych. Już obecnie istnieje wiele technologii które zmieniają sposób w jaki ludzie podejmują decyzje, robią zakupy, działają w biznesie. Im więcej jest dostępnych danych, tym bardziej kompletną decyzję można podjąć. Wokoło nas jest wiele informacji które nie są sformatowane w znaczący, sensowny dla człowieka sposób. W e-handlu bazującym na IoT sformatowana informacja pozwala na podejmowanie odpowiednich decyzji dotyczących np. produkcji i dostępności towarów on-line.

Inteligentne miasto to zarówno pożyteczna infrastruktura, ale przede wszystkim miejsce życia ludzi (Forth 2015). To życie musi być znośne a może nawet wygodne (Seta 2016). Inteligentne miasto jest projektem rozwojowym integrującym technologie ICT i IoT, oraz wiele innych, w taki sposób aby łączyć poszczególne obszary działania jednostek, organizacji, instytucji, funkcjonalności, usług i infrastruktury w pewną całość poprawiającą bezpieczeństwo, jakość życia, wygodę, sprawność energetyczną i informacyjną, zapewniającą ciągłość działania systemów funkcjonalnych, poprawiającą i rozszerzającą sferę usług, i wiele innych. Obecnie nie ma jednolitej koncepcji inteligentnego miasta. Wymienia się natomiast szereg niezbędnych elementów z czego wyłania się przyszła koncepcja tak bardzo skomplikowanego tworu. Wśród elementów tworzących inteligentne miasto badane są warstwy ogólne określane jako niezbędne: mieszkańcy tworzą społeczność opartą na wiedzy, jednostki, instytucje i procedury tworzą wiedzę, zarządzają, weryfikują i korzystają z niej, posiadają zdolność do innowacji, adaptacji i rozwiązywania nowych problemów. Inteligentne miasto to struktura zapewniająca rozwój kapitału ludzkiego i społecznego, ułatwiająca działalność gospodarczą, ukierunkowane na zrównoważony rozwój. Inteligentne miasto to w żadnym wypadku obóz koncentracyjny dla w różny sposób monitorowanych ludzi wypełniony super-infrastrukturą i zarządzany super-inteligencją. Inteligentne miasto to przede wszystkim sposób jego organizacji, rodzaj warstwy humanistycznej, a dopiero dalej technika. Podobnie jak wymieniano poprzednio w odniesieniu do ogólnych atrybutów IoT, inteligentne miasto wyposażone jest w zaawansowaną sieć telekomunikacyjną, sprawne municypalne systemy funkcjonalne, znaczną liczbę czujników i sieci czujnikowych, sterowniki urządzeń, specjalizowane bazy danych, systemy wspomagania decyzji, inteligentne fragmenty infrastruktury miejskiej jak inteligentne domy, ulice, oświetlenie, energetykę, zaopatrzenie w wodę, gospodarkę odpadami, itp. Obecne prace badawcze i rozwojowo wdrożeniowe w obszarze inteligentnego miasta dotyczą budowy i testowania różnych fragmentów takiego ogólnego projektu w aspektach sprzętowym i oprogramowania, opcji rozwojowych, architektonicznych a także integracji poprawionych czy nowych funkcjonalności z różnymi formami infrastruktury miejskiej. Korea Południowa realizuje niezwykle ambitny projekt ultranowoczesnego miasta biznesowego Songdo, nazywanego ubiquitous city. Można podać setki przykładów takich mniejszych i większych testów rozwiązań pilotowych. Spora część prac dotyczy budowy systemów video, akwizycji takich danych, zarządzania nimi w sensie umiejętności sprawnego wyboru informacji użytecznych z wielkich zbiorów danych cyfrowych. Duża część prac dotyczy nowych algorytmów zarządzania systemami miejskimi. Bodajże największa część prac dotyczy rozmaitych pożytecznych rozwiązań czujnikowych usprawniających działanie miasta lub nadających infrastrukturze nowe funkcjonalności. W zakresie bezpieczeństwa i kontroli ruchu drogowego i transportu prowadzone są prace nad badaniem zmian schematów i struktur ruchu od skali całego miasta, nawet do poziomu pojedynczego pojazdu. Zapisywane są i analizowane wzorce ruchu pojazdów i ich rodzaju, wzorce i natężenie ruchu pieszych, itp. Obliczane są wzorce średnie i zależności statystyczne. Tworzone są modele przemieszczania się pojazdów i ludzi. Na tej podstawie optymalizowane są parametry transportu publicznego, świateł drogowych, itp. Celem jest zmniejszenie zużycia energii, paliwa, czasu oczekiwania na transport, zmniejszenie zanieczyszczenia i zatłoczenia ulic, itp. Przedmiotem dodatkowych analiz są znaczne odstępstwa od średnich wzorców ruchu i ich przyczyny, także wpływ pogody, wielkich imprez masowych, wydarzeń niespodziewanych, wypadków, itp. Prowadzone są testy wyposażania elementów ‘umeblowania’ miejskiego, małej infrastruktury i architektury miejskiej związanej z ruchom drogowym i parkingami w czujniki dodające tym miejscom dodatkowe specjalizowane funkcjonalności np. związane z bezpieczeństwem, ale także z informacją dotyczącą użytkowania, informacją turystyczną o obiekcie, itp. Lokalny system radiowy obiektu łączy się z aplikacją w komórce turysty i wyświetla dodatkowe informacje. Prowadzone są prace nad wieloma funkcjonalnościami małej architektury miejskiej, które wydają się dzisiaj śmieszne. Wiele z takich projektowanych funkcjonalności wymaga zaangażowania jedynie bardzo małych zasobów technicznych w tym głównie transmisji danych i zapotrzebowania na energię. Znaki drogowe i słupki parkingowe wytyczające obszary, czy ograniczające dostęp dla samochodów są wyposażane w czujniki zbliżenia, liczniki, mikrofony i głośniki, czujniki dymu i ognia, a niektóre w proste kamery, ale włączane tylko w specyficznych sytuacjach. Dane z mikrofonu nie są przesyłane dalej jeśli są typowe np. rejestrują ‘szum miasta’, zresztą ten szum analizując spektralnie i jego długoczasowe zmiany. Ale jeśli jest to dźwięk nietypowy np. wystrzał, krzyki, dźwięk uderzenia, klaksonu, itp. Dane takie mogą podnosić specyficzne alarmy w lokalnej centrali i np. włączać kamerę lub zawiadamiać służby miejskie. Ktoś by dzisiaj powiedział, że niestety zakres inwigilacji rośnie. Par-

komaty wymagające podawania numeru rejestracyjnego samochodu wzbudziły ostatnio w Warszawie wiele protestów. Kiedyś nie będziemy tego prawdopodobnie zauważać i traktować jak coś naturalnego. Chyba że rozwój pójdzie w innym kierunku.

Inteligentne rolnictwo, produkcja żywności, leśnictwo, zagospodarowanie i ochrona środowiska naturalnego są obszarami ingerencji IoT. IoT będzie najprawdopodobniej najszybciej zmieniał produkcję żywności. Precyzyjne i inteligentne rolnictwo i leśnictwo podąża w kierunku pełnej automatyzacji i ograniczenia w maksymalnym stopniu bezpośredniej pracy człowieka, tam gdzie jest to tylko możliwe. IoT dostarcza danych dla rolnictwa precyzyjnego i inteligentnego niezbędnych do optymalizacji gospodarowania. Brane są także pod uwagę zastosowania IoT przeciwdziałające zagrożeniom dla rolnictwa i środowiska naturalnego wprowadzanym przez zmiany pogody i przez rozwój cywilizacji. Spotyka się także nie odosobnione opinie, że wielkotowarowa produkcja żywności w przyszłości ze środowiskiem naturalnym i klasycznie rozumianym rolnictwem będzie miało coraz mniej wspólnego. Autonomiczne ciągniki rolnicze, wyposażone w wiele czujników, już dzisiaj produkuje i testuje w serii koncepcyjnej, a wkrótce sprzedaje firma CASE (www.caseih.com). Na portalu youtube można zobaczyć kilka imponujących filmów demonstracyjnych tego ciągnika zdolnego do nieprzerwanej pracy przez dziesiątki godzin. W portalu firmy zamieszczone są dane techniczne i charakterystyki autonomicznego ruchu kilkutonowego traktora, w tym rozwiązania dotyczące bezpieczeństwa eksploatacji, dokładności ruchu koordynowanego sygnałem GPS, omijaniem przeszkód niespodziewanych, planowaniem pracy, procedurami związanymi z utratą sygnału, współpracą z ciągnionymi i także inteligentnymi maszynami rolniczymi, itp. Podobieństwo tego ciągnika, wykonanego w znacznie mniejszej skali, do tych przedstawionych w filmie Interstellar być może sugeruje inspirację. Rolnictwo precyzyjne wykorzystuje wyposażony w czujniki ciągnik mierzący rozkład właściwości gruntu np. metodą LIBS i ustalający konieczność nierównomiernego rozkładu nawożenia, szczególnie azotu, ale także fosforu i potasu. Specjalistyczne rozkładalne po pewnym czasie mikro-czujniki mogą być także rozsiewane na znacznych obszarach dając precyzyjne mapy właściwości gleby. Dane do analizy obrazowej plonów, zagrożeń chorobowych roślin, rozsiewania środków ochrony roślin, i wiele innych parametrów i zjawisk jest gromadzonych prostym sposobem przez specjalizowane drony rolnicze. Szybko uzyskane adekwatne wyniki pomiarów umożliwiają interwencję w czasie rzeczywistym. Natychmiastowa analiza DNA i roli patogenów na miejscu uprawy umożliwia adekwatną reakcję biochemiczną naprawy. Obecnie przenośne laboratorium analityczne z sekwencerem DNA wykonuje takie zadania w mniej niż godzinę w warunkach polowych. Synteza DNA drożdży, znacznie poprawionych genetycznie, i wykonujących swoje klasyczne zadania, jest prawie opanowana. Jako wymowny i nieco futurystyczny przykład zastosowania IoT ingerującego w przyrodę podaje się koncepcje zastosowania cyber-owadów IoT do zapylania roślin, jeśli pszczoły w przyszłości nie wytrzymałyby zmian środowiska, byłoby ich za mało, lub odmówiłyby całkowicie współpracy. Rozważane koncepcje to opracowanie mikro-dronów lub ingerencja w relatywnie prosty system nerwowy dużych owadów np. takich jak ważki. Dla mikro-dronów na razie nie istnieją kompatybilne źródła energii i na widocznym horyzoncie technicznym na razie takich źródeł nie widać. Oznacza to, że jest to sprawa na kilka dziesięcioleci, chyba że nastąpi niespodziewany przełom w zakresie wydajnych i pojemnych źródeł energii, w szczególności sub-miniaturowych. W drugim przypadku, dość zaawansowana elektronika o wadze miligramów zdolna do realizacji złożonych algorytmów i przetwarzania dużych ilości danych istnieje już dzisiaj i testy na większych owadach, jak ważki, i innych zwierzętach są prowadzone. Liczba owadów potrzebnych do zapylania roślin jest tak duża, że projekt należy raczej do sfery szybko nie realizowalnych. Ewentualnie nadzieja że uratują nas cyberowady jest chyba dość naiwna. Natomiast badania nad minidronami o wadze dekagramów, mikrodronami o wadze gramów i nanodronami o wadze miligramów, operującymi w otoczeniu człowieka, w pomieszczeniach gdzie przebywa człowiek są bardzo interesujące i prowadzone przez wiele laboratoriów, np. DARPA. Jeden z nurtów prac dotyczy mikrodronów bio-mimetycznych z trzepoczącymi skrzydłami jak u kolibra, trzmielaka czy ważki. Demonstracje działania takich urządzań można znaleźć łatwo na Internecie. Ich potencjalne zastosowania są bardzo szerokie i dotyczą także penetracji miejsc niedostępnych, bezpieczeństwa, ukrytego monitoringu, skoordynowanego działania w stadach. Demonstracje przygotowane przez laboratorium AFRL są dość przerażające. Mówi się także o fotowoltaicznych dronach telekomunikacyjnych jak NASA Pathfinder, latające praktycznie bez przerwy na wysokości ponad 20 km i zastępujące satelity geostacjonarne. Warto zdawać sobie sprawę do czego zdolne są takie urządzenia IoT już obecnie i w dalszej przyszłości. Obszar potencjalnej penetracji IoT w zagospodarowanie środowiska, leśnictwo, rolnictwo i przemysł spożywczy jest znaczny. Obejmuje np. zastosowanie autonomicznych maszyn rolniczych, automatyzację procesów wytwórczych żywności, kontrolę jakości, powszechny i wszechobecny monitoring środowiska naturalnego i wiele innych.

Energia jest nieodzownie potrzebna człowiekowi i jego cywilizacji. Brak energii cofnąłby nas natychmiast znacznie wstecz w rozwoju. To właśnie stopień ‘ujarzmienia’ energii decyduje o stopniu rozwoju naszej cywilizacji. Można powiedzieć, że jest to główny i jednoparametrowy wskaźnik naszego rozwoju. IoT zmienia obszar energii. Zagadnienie energii, źródeł energii, stałych i mobilnych, szczególnie wielka i mała energetyka, energetyka odnawialna, zbieranie energii ze środowiska, oszczędzanie energii, optymalizacja użycia energii, i tzw. energetyka mobilna to kluczowe zagadnienia do dalszego rozwoju cywilizacji, a także wielu z dziedzin IoT. Niska relatywnie wydajność fotowoltaiki nie jest nadmierną przeszkodą w stworzeniu w przyszłości infrastrukturalnego systemu energetycznego jeśli elementy są tanie i zajmują ogromne powierzchnie. Tym bardziej jeśli takie powierzchnie nie przeszkadzają, nie zajmują miejsca na rolnictwo i budownictwo. Te powierzchnie nie mogą być cennymi terenami rolniczymi. Te powierzchnie muszą być związane z obszarami zurbanizowanymi. Narzucają się drogi bitumiczne i dachy. I takie właśnie rozwiązania są testowane nie tylko w laboratoriach ale także praktycznie. We Francji uruchomiono testowy odcinek drogi fotowoltaicznej. W Izraelu testowana jest przez firmę SolarPaint gęsta farba fotowoltaiczna do nakładania na dowolne powierzchnie, w tym drogi, dachy, ściany budynków. Powierzchnia dróg to tysiące kilometrów kwadratowych zdobywanej relatywnie tanio energii jeśli asfalt przyszłości będzie fotowoltaiczny. Oprócz badań nad fotowoltaiczną nawierzchnią dróg prace są prowadzone także nad fotowoltaicznymi dachówkami. Oprócz fotowoltaiki mówi się o modnej dzisiaj energetyce ruchomej. Energetyka ruchoma to taka która jest związana z człowiekiem, pojazdami, urządzeniami autonomicznymi. Taka energetyka, w celu poprawienia funkcjonalności będzie usieciowiona w celu wyrównywania poboru i użycia oraz oddawania trudnego do magazynowania nadmiaru energii. Energetyka w wielkiej skali będzie w przyszłości prawdopodobnie fuzyjna. Europa stawia na rozwiązania fuzyjne a nie rozszczepialne, inwestując znaczne środki finansowe i potencjał naukowy w projekty ITER i DEMO. Pierwsza elektrownia fuzyjna DEMO ma być uruchomiona w roku 2050 w Cadarache. Warunkiem jest opanowanie problemów technicznych fuzji plazmy wysokotemperaturowej, a także bezpiecznego przesyłania i zarządzania metodami IoT wielkimi ilościami energii. Na przykład, dla energetyki termojądrowej testowane muszą być materiały długoterminowo odporne na promieniowanie neutronowe. Badania będą trwały wiele lat. Takich materiałów nie ma, ale mniej więcej wiadomo dzisiaj gdzie ich poszukiwać. Zapotrzebowanie na energię będzie ciągle rosło. Rozwiązanie tego problemu jest kluczowe dla przyszłości energetyki globalnej, jak się ocenia w najbliższym 30-40-leciu. IoT ma także pomóc w racjonalizacji zużycia energii. Sektor energetyki podlega obecnie najintensywniejszym procesom przemiany i cyfryzacji spośród innych sektorów przemysłowych. Inteligentna energetyka jest obecnie jedną z najbardziej przetransformowanych obszarów w kierunku IoT. Wiele stacji energetycznych jest w pełni skomputeryzowanych i usieciowionych. Modernizowane są funkcjonalne stacje i słupy energetyczne średniego napięcia, wyposażane w czujniki prądów, napięć, temperatury, monitoring bezpieczeństwa, kamery video. Z rozległymi sieciami energetycznymi związane są problemy bezpieczeństwa, rozproszonych brzegowych sieci czujnikowych i sterownikowych IoT, inteligencji środowiska pracy energetyki, serwisowanie odległych obszarów, itp. Energetyka mobilna jest związana z postępami w technologii baterii i akumulatorów. Optymalne wykorzystanie mobilnych zasobów związane jest z usieciowieniem indywidualnych ruchomych magazynów energii. Akumulatory i baterie, większe i mniejsze, będą miały interfejsy do IoT.

Cyberbezpieczeństwo jest relatywnie nową kategorią uzupełniającą w nowy ilościowy i jakościowy sposób ogólną kategorię bezpieczeństwa. Wiele z elementów cyberbezpieczeństwa dotyczy bezpośrednio człowieka, a część infrastruktury (Elbaz 2017), (Russel 2016), (Etter 2016). Człowiek jako użytkownik bierny i aktywny IoT, popełniający błędy, poruszający się w sieci czasami chaotycznie jest narażony na związane z cyberbezpieczeństwem szkodliwe działania rozproszone, infrastrukturalne, lokalne, intencjonalne. Co chwila dowiadujemy

się o nowych metodach 'polowania' na użytkownika Internetu, w tym także IoT. Niedawno plagą był wirus Locky, i jego znany duystrybutor Necurs botnet, typu ransomware szyfrujący dane użytkownika i wymuszający okup za odszyfrowanie. Obrzydliwym przykładem takiego działania było żądanie wysokiego okupu od szpitali amerykańskich Hollywood Presbyterian Centre, Kentucky Methodist Hospital, Chino Valley Medical Center i Desert Valley Hospital w Kaliforni. W popularnych aplikacjach np. Sklep Play pojawiają się aplikacje pułapki. Np. ostatnio taką aplikacją była Flashlight Widget, pozornie niegroźna latarka na Androida wykradająca dane użytkownika z telefonu. Zagrożenie dla infrastruktury obsługiwanej przez IoT jest także poważne gdyż zmasowany atak może prowadzić potencjalnie do katastrofy o poważnych skutkach lokalnych i globalnych. Wiele aktualnych komentarzy dotyczących cyberbezpieczeństwa, a w tym najważniejszych zagrożeń dla IoT jest publikowanych na portalu DARKReading. A dzieje się w tym obszarze wiele, np. bezplikowe ataki malware, kradzieże identyczności encji IoT, spamowanie IoT, analiza masowości zagrożeń IoT, działania organizacji społecznościowej OWASP – open web application security project publikującej okresowo listę Dziesięć Głównych Wrażliwości – Top Ten Vulnerabilities, działania oddziału DISA – Defense Information Systems Agency – rządowego departamentu DoD, przygotowania administracji rządowych niektórych krajów do masowej kontroli IoT, i wiele innych. W odniesieniu do IoT mówimy najczęściej o następujących czterech nieco różnych kategoriach bezpieczeństwa, nazywanych kwadrupolem zaufania PSPS w cyberprzestrzeni: protection, security, privacy oraz safety, czyli zabezpieczeniu, ochronie, prywatności i bezpieczeństwie (Thampi 2014). Tutaj interesuje nas głównie bezpośrednie i pośrednie bezpieczeństwo i ochrona człowieka. Postępujące usieciowienie domów, miast, infrastruktury municypalnej, biznesu i przemysłu, systemów energetyki i ogrzewania, ruchu drogowego, także małej infrastruktury i przedmiotów użytkowych niesie w sobie wiele nowych zagrożeń. Niektóre z tych zagrożeń mogą dotyczyć bezpośrednio życia i zdrowia człowieka, niektóre przemysłu wytwórczego, inne mogą nieść zagrożenia globalne. Niedawno temu unieruchomienie części systemu energetycznego w kraju europejskim blisko naszych granic odbyło się na drodze programistycznej po wrogim przejęciu kontroli nad wieloma podstacjami energetycznymi. W Polsce zdecydowano ostatnio o organizacji centralnej instytucji zabezpieczenia energetyki. Koszty jej organizacji oceniane są na niewielki procent kosztów zniszczeń potencjalnego ataku. Największy dotychczas zidentyfikowany botnet IoT wykorzystujący malware o nazwie Mirai grupy NWH, poprzez zmasowany atak DDoS na serwery DNS amerykańskiej firmy internetowej DYN w dniu 21.10.2016, spowodował czasowe zablokowanie usług wielu milionom ludzi w Ameryce Północnej i Europie. Botnet został prawdopodobnie utworzony z sieci wielu zainfekowanych urządzeń podłączonych do Internetu takich jak drukarki, kamery internetowe, sieciowe rutery abonenckie, sieciowe urządzenia nadzoru, obszarów, przedmiotów i ludzi, itp. Można sobie wyobrazić podobne i znacznie bardziej niebezpieczne ataki unieruchamiające lub nawet uszkadzające w sposób katastrofalny znaczne części krytycznej infrastruktury np. związanej z informacją, transportem, finansami, energetyką, opieką zdrowotną, zaopatrzeniem w wodę, itp. Coraz częściej zdarzają sięataki o zasięgu globalnym. Ostatnio, w maju 2017 taki atak przeprowadzony był w Europie. Po ataku Mirai po raz pierwszy użyto w prasie technicznej terminu Internet Rzeczy Niekoniecznych, kontestując w ten sposób konieczność podłączania już obecnie do Internetu takich rzeczy jak pralek, lodówek, pryszniców, zmywarek do naczyń, czajników, budzików, suszarek do włosów, czytników e-booków, różnego rodzaju alarmów, zamków do drzwi, prostych urządzeń dostępowych, lokalizatorów dla dzieci ale także dla psów i kotów, oraz szczoteczek do zębów i wycieraczek do butów. Wszystkie te wymienione przedmioty, relatywnie małe i tanie, wyposażone w najprostsze niezabezpieczone interfejsy IoT są potencjalnie bardzo podatne na bezpośrednią czy pośrednią infekcję szkodliwym oprogramowaniem wirusowym. Przez takie urządzenia możliwy jest w niektórych przypadkach dostęp do sieci lokalnej i następnie wyższego rzędu. Rozwinęła się także w prasie popularnej dyskusja dotycząca różnych kategorii Internetu Rzeczy Niepewnych w sensie bezpieczeństwa, Niepotrzebnych, Niekoniecznych, Zbędnych i Bez Sensu, oraz nad różnicami pomiędzy tymi kategoriami. IoT ma gorących zwolenników, ale także zagorzałych przeciwników, i to wcale nie głównie antyglobalistów, przeciwników nowej groźnej, nieprzyjaznej człowiekowi cywilizacji globalnej stojącej ponoć za IoT. Szerszy opis tego 'niechcianego' sektora IoT można łatwo znaleźć pod hasłami Internet of NoThings, The Internet of Insecure Things, a także The Internet of Unnecessary Things, czy The IoT we do not need. Na szczęście intensywne działania w obszarze cyberbezpieczeństwa ICT i IoT są prowadzone na wielu płaszczyznach. Zaangażowani są producenci urządzeń brzegowych IoT, czujników, interfejsów, sieci, chmury, baz danych, oprogramowania, itp. Tematyka jest bardzo szeroka i przekracza ramy niniejszego opracowania. Można wymienić przykładowo niektórych liderów technologii cyberbezpoieczeństwa IoT: wolfSSL, DataFloq, Toothless, Aries embedded, SSRN, IPA, Trusted Computing Group oraz wprowadzany standard układu scalonego bezpieczeństwa TPM – trusted platform module, i wiele innych. Być może standard TPM stanie się obowiązkowy w niedalekiej przyszłości w urządzeniach ICT i IoT. Otwarta, niedochodowa organizacja społecznościowa OWASP, którą wymieniono już powyżej (owasp.org), posiadająca wiele tysięcy aktywnych użytkowników wiki, youtube, vimeo i innych, działa na rzecz 'wizualizacji' bezpieczeństwa oprogramowania. OWASP jest neutralna względem producentów oprogramowania i nie wspiera produktów komercyjnych. Opracowywane oprogramowanie i dokumentacja techniczna dotyczy oceny poziomu cyberbezpieczeństwa i zwiększenia świadomości użytkowników w tym obszarze. OWASP posiada lokalny oddział w Polsce. Podobny charakter działania ma członkowskie Stowarzyszenie (ISC)[2] – Inspiring Safe and Secure Cyber World, które wydaje znane i powszechnie akceptowane i cenione przemysłowe certyfikaty bezpieczeństwa dotyczące administracji IT, chmury i operacji systemów w biznesie i przemyśle – SSCP, CCSP i SISSP. Znane i aprobowane certyfikaty A+, Network+ i Security+ wydaje także Stowarzyszenie przemysłowe CompTIA – Computing Technology Industry Association. Autoryzowane szkolenia CompTIA odbywają się także w Polsce.

Systemowe rozwiązanie bezpieczeństwa IoT w skalach lokalnej i globalnej jest zagadnieniem trudnym, i przede wszystkim bardzo kosztownym. Kosztownym dlatego, że do tej pory rozważano zagadnienia bezpieczeństwa IoT, o ile w ogóle, osobno od urządzeń i systemów. Przyszedł czas na pełną integrację warstwy bezpieczeństwa z tymi urządzeniami. Koszty bezpieczeństwa w pewnym sensie znikną, wbudowując się w urządzenie, którego nie można będzie wypuścić na rynek baz zapewnienia standaryzowanego poziomu bezpieczeństwa. Rekomendowany przez specjalistów np. Fundację prpl dokument Security Guidance jest sformalizowną listą czynności wymaganych np. do poprawnego zabezpieczenia inteligentnego domu bazującego na IoT. Lista jest długa i zawiera takie rekomendacje jak: regularną aktualizację firmware rutera abonenckiego, częstą zmianę administracyjnego hasła dostępu do rutera, optymalną konfigurację polityk firewall a w tym zamykania nieużywanych portów, używanie funkcji filtrowania numerów sprzętowych MAC, konfiguracja sieci gościnnej dla urządzeń gości, bezpieczna konfiguracja funkcjonalności WPA/WPS serwera dostępowego, aktywacja izolacji dostępu bezprzewodowego, dezaktywacja ustawiania DNS poprzez DHCP, dezaktywacja udostępniania plików poprzez USB, dezaktywacja funkcjonalności UPnP, i wiele innych. Jeśli takie procedury nie będą zautomatyzowane to przeciętny abonent IoT raczej nie zapewni sobie odpowiedniego poziomu bezpieczeństwa. Wielu niezabezpieczonych abonentów naraża nieświadomie na niebezpieczeństwo cały system, ale także siebie osobiście. Ta niepełna lista to jest tylko część odpowiedzialności po stronie abonenta, w żadnym wypadku nie wyczerpująca bezpieczeństwa systemu IoT. Operator IoT musi zdjąć niektóre z wymienionych obowiązków z abonenta, jeśli system ma być bezpieczny. Silną motywacją do szukania kompleksowych rozwiązań cyberbezpieczeństwa abonenta jest ciągle, aż do znudzenia, powtarzane hasło w mediach popularnych i społecznościowych „wszystko co robisz w sieci, lub za ciebie robią, zostanie wykorzystane przeciwko tobie". Zagadnienia bezpieczeństwa posiadają inną skalę i inne problemy w przypadku różnych odmiennych warstw IoT – abonenckiego, usługowego, przemysłowego i biznesowego oraz infrastrukturalnego. Przejęcie kontroli nad wodociągami, energetyką miejską czy oświetleniem ulic w nocy ma inną wymowę niż zatrzymanie produkcji w fabryce, przejęciem tajemnic biznesowych i finansowych firmy, czy zatrzymaniem funkcjonalności inteligentnego domu, lecz we wszystkich przypadkach może być w inny sposób bardzo niebezpieczne. Odpowiedzialność za bezpieczeństwo IoT jest wielowarstwowa ze skomplikowanym przeplataniem i nakładaniem się warstw. Odpowiedzialność ta nie kończy się na granicy państwa. Musi posiadać silny składnik międzynarodowy, uwzględniający jednak w jakiś sposób suwerenność. System bezpieczeństwa IoT nie może być homogeniczny, w prosty sposób scentralizowany. Musi dysponować wieloma różnorodnymi narzędziami analitycznymi działającymi na różnych poziomach, warstwach i domenach sieci. Państwo posiada odpowiednie siły i środki i odpowiada globalnie

za bezpieczeństwo systemów sieciowych dla edukacji, administracji, ochrony zdrowia, zapewnienia odpowiednich warunków bezpiecznego i efektywnego gospodarowania, infrastruktury, itp. Każdy poziom ma swoją odmienną rolę w zapewnieniu bezpieczeństwa jak operatorzy, samorząd lokalny, jednostki gospodarcze, indywidualni użytkownicy. Co w zakresie cyberbezpieczeństwa IoT robi nauka? Próbuje antycypować potencjalne zagrożenia, klasyfikować i oceniać ich wagę. Próbuje badać odporność IoT na wojnę informacyjną, cyberwojnę o niewyobrażalnych konsekwencjach. Jednym z najsłabszych punktów jest wielka różnorodność bezprzewodowych sieci czujnikowych. Czujniki w takich sieciach dostarczają kluczowych informacji masowych wykorzystywanych po przetworzeniu do podejmowania decyzji, a także do tworzenia wiedzy. Przejęcie kontroli nad takimi sieciami czujników umożliwia wstrzyknięcie w system fałszywych lecz uwiarygodnionych informacji lub wykorzystania informacji czujnikowych do podejmowania własnych decyzji wyprzedzających. Możliwości tutaj jest wiele, jak np. intencjonalne doprowadzenie do katastrofy przemysłowej. Analizowane są różne przypadki modelowe. Niektóre z tych analiz dotyczą przejęcia kontroli nad oprzyrządowaniem czujnikowym smartfonów, a w szczególności np. nad akcelerometrem, kompasem, żyroskopem, lokalizatorem. Dane z tych czujników dostarczają nadspodziewanie wielu informacji o użytkowniku smartfonu. A jeśli telefon jest dodatkowo połączony ze smartwatchem to uzyskujemy dość dokładny obraz rodzaju ruchu i zachowania właściciela, łącznie z jego tętnem, częstością oddechu, średnią długością kroku, niektórymi przyzwyczajeniami, itp. Przemysł natomiast poddaje pod dyskusję możliwość opracowania znormalizowanych wytycznych dotyczących bezpiecznego użytkowania konsumenckich urządzeń IoT, a także wdrażania ścisłych norm dla infrastrukturalnych urządzeń IoT.

Bezpieczeństwo i cyberbezpieczeństwo jest pojęciem wielowymiarowym. Dotyczy działania poszczególnych urządzeń, infrastruktury, człowieka i całych społeczeństw. Posiada aspekty techniczne, cywilne, prawne, militarne, globalne, i wiele innych. IoT będzie odgrywał bez wątpienia istotną rolę w wielu z tych poziomów i obszarów dotyczących bezpieczeństwa. Przewiduje się, że IoT będzie ogólnie dbał sam z siebie o bezpieczeństwo. IoT staje się, a właściwie już jest, jednym z potencjalnych teatrów działań militarnych. Indywidualne kraje zapewniają bezpieczeństwo wielopoziomowo. Koordynatorami są instytucje centralne, np. w Holandii Narodowe Centrum Cyberbezpieczeństwa NCSC. W innych krajach jest podobnie, powoływane są instytucja centralne. W Polsce jest to kilka instytucji, a w tym Narodowe Centrum Kryptologii, Ministerstwo Cyfryzacji, MON, ABW, itp. Bezpieczeństwo globalne, pomijając sprawy polityczne i wojskowe, jest związane z epidemiologią i obserwacjami medycznymi, katastrofami naturalnymi i obserwacją środowiska, katastrofami infrastruktury i spowodowanymi przez człowieka, a także np. obserwacjami kosmosu i w przyszłości także dostatecznie wczesnym zabezpieczeniem przed kolizją z planetoidami. Znana jest mniej więcej statystyka takich zagrożeń. Kiedyś nic na to nie mogliśmy poradzić. Dzisiaj jesteśmy nieco bliżej, choć jeszcze daleko, od aktywnej obrony. Obrona będzie bazować przede wszystkim na robotycznych obserwacjach całego nieba i zbieraniu danych o zagrożeniach. Tym bardziej, że takie zagrożenie może mieć charakter terminalny dla całej cywilizacji. Podobne zagrożenie może pochodzić od sterylizującego impulsu promieniowania generowanego w niewielkiej odległości od Ziemi. Bardzo istotne mogą okazać się globalne zagrożenia epidemiologiczne, przed którymi ostrzegał niedawno Bill Gates w czasie ostatniego Światowego Forum Ekonomicznego w Davos, związane ze wzrastającą odpornością bakterii na antybiotyki i ogromną niekontrolowaną mobilnością ludzi. Najpoważniejszym czynnikiem zagrożenia jest związana z tym znaczna szybkość potencjalnego rozprzestrzeniania się epidemii, oceniana na tygodnie a nawet dni w najgorszych scenariuszach. Natychmiast reagujące brzegowe technologie IoT, wyposażone w inteligencję obliczeniową, rozproszone w całej sieci funkcjonalnej i dodatkowo ruchome w postaci różnych, trudnych do zidentyfikowania agentów bezpieczeństwa mogą odegrać fundamentalną rolę w systemach bezpieczeństwa lokalnego i globalnego. Indywidualny użytkownik IoT także będzie mógł aktywować i posiadać swojego agenta bezpieczeństwa.

IoT jest współ-generatorem kompleksowych zmian w baranży finansowej. Branża bankowa uznaje potencjał takich bezpiecznych technolgii jak blockchain i kryptowalut, widząc w nich poważnego konkurenta dla obecnego status quo i dalszego utrzymania technologii klasycznych. Stąd wynika, że należy oczekiwać istotnych zmian (Skinner 2016), (Hishti 2016). Utrzymywanie obecnego status quo systemu finansowego na dłuższą metę nie uda się. Wypchany gotówką portfel musi odejść do lamusa. Już przeważają transakcje elektroniczne. Zaczynamy posiadać wirtualne portfele. Przechodzimy w etap społeczeństwa bezgotówkowego. Jednocześnie zwiększa się kontrola państwa nad finansami. Powstaje nowa branża nazywana FinTech łącząca technologie ICT, IoT i finanse (Capgemini 2016). Podobnie dzieje się w sektorze ubezpieczeń, gdzie mówimy o nowej generacji systemów InsurTech. Powstałe w 2015 roku konsorcjum FinTech obejmuje największe banki świata jak: BoA, Citi, Societe Generale, DB, Barklays, JP Morgan, ING, HSBC, Goldman Sachs, Barclays, i Credit Suisse. Niektóre banki, jak Citi z Citicoin, wprowadzają swoją walutę, konkurencyjną do bitcoin. Blockchain znakomicie nadaje się do rozliczania transakcji kupna-sprzedaży w wielu branżach komercyjnych i przemysłowych. Tematyka roli i udziału IoT w rozwoju sektora finansów jest bardzo szeroka i rozwija się dynamicznie. Używane są gdzieniegdzie terminy Internet of Value IoV, Finternet of Things, lub FIoT. Celem jest budowa globalnego systemu, który pozwoli na transakcje, przesyłanie, akwizycję, obrót, itp., różnymi aktywami wartościowymi w sieci jak: akcje, instrumenty i produkty finansowe, produkty ubezpieczeniowe, bony, instrumenty lojalnościowe, itp. Blockchain to początek głębokich przemian. Zaczynamy od utrzymania wspólnej, w pełni cyfrowej, zbiorowej księgi rachunkowej transakcji pomiędzy komputerami. Księga jest rozproszona po całej sieci w takich samuych kopiach w pełni zabezpieczonych kryptograficznie. Użytkownik ma dostęp do swoich transakcji. W odniesieniu do roli IoT w usługach finansowych mówi się o następujących podstawowych warstwach funkcjonalnych: prywatności, bezpieczeństwie, zarządzaniu identyczności, interoperacyjności, współpracy, personalizacji oraz niezawodności. Omówienie tej ciekawej problematyki wykracza poza ramy tej pracy.

Konsumpcja zawartości medialnej i rozrywkowej wzrasta na platformach cyfrowych i mobilnych. Wzrost rynku medialnego i rozrywkowego IoT, według szacunków Verizon i TCS – Tata Consultancy Services, wynosi obecnie kilkadziesiąt procent rocznie, co lokuje ten sektor IoT globalnie na trzecim miejscu w szybkości wzrostu po produkcji oraz finansach i ubezpieczeniach. Pod względem kwotowym sektor medialny i rozrywkowy IoT nie jest jeszcze znaczny i lokuje się podobnie do sektora podróże, transport i hotelarstwo. Główny wzrost sektor medialny zawdzięcza rozwojowi aplikacji mobilnych i możliwości zbierania danych o klientach przez interesariuszy i dostarczycieli usług. Wpisując się w terminologię IoT sektor nazywany jest The IMET – Internet of Media and Entertainment Things. Sektor obejmuje wszelkiego rodzaju przedsiębiorstwa medialne i rozrywkowe jak wydawnictwa, publikatory, nadawcy, dostarczyciele usług, agencje reklamowe i marketingowe, firmy informacyjne, producenci elektroniki konsumpcyjnej, studia telewizyjne i filmowe, organizacje sportowe, obiekty rekreacyjne, promotorzy i organizatorzy wydarzeń, koncesjonerzy gier losowych, kasyna, i wiele innych. Sektor rozwija się dzięki rozwojowi szerokopasmowej infrastruktury transmisyjnej i nowym formatom jak 3D, 4D, 4K, UHD, HDR, VR, 5G, DLNA, itp. Kluczem do rozwoju, obok mobilności, wydaje się być personalizacja usług. W nieco dalszej perspektywie będzie to także segment elektroniki ubieralnej zdolnej do dostarczania mediów.

Paradygmat IoT zastosowany w odniesieniu do dziedzictwa kulturowego, i w oczywisty sposób głęboko dotykający człowieka, jest relatywnie nową koncepcją integrującą wszystkie możliwości tej coraz bardziej wszechobecnej technologii w odniesieniu do statycznych miejsc kultury. Nie trudne było do przewidzenia, że IoT obejmie także kulturę wysoką, tą statyczną, architektoniczną, historyczną, archeologiczną, miejsca kultu, pomniki, muzea, wystawy, do której cały czas pielgrzymują milionowe rzesze ludzi, jak i tą dynamiczną prezentowaną w teatrach, salach koncertowych i wystawowych, operach i filharmoniach. Zadaniem IoT jest subtelna transformacja dziedzictwa kulturowego w inteligentne środowisko – Internet Rzeczy Kultury, Internet Dziedzictwa Kulturalnego. Zawsze relacje kultury wysokiej z mediami, technologiami i usługami popularnymi, wszechogarniającymi były dość skomplikowane i raczej powściągliwe. Tak jest i tutaj. Mamy nadzieję, że twórcom IoT Kultury uda się opanować pozytywnie spontaniczność i dynamikę rozwoju i aplikacji tej przenikliwej technologii w tym ważnym społecznie obszarze naszego życia. IoT Kultury, jeśli odpowiednio stosowany, ma szansę wprowadzić nowe wartości, stworzyć rodzaj twórczych e-kuratorów kultury i sztuki. Promocja wysokiej kultury statycznej będzie musiała być przemyślana od nowa, wprowadzając tą kulturę w zrównoważone, trwałe, powszechnie dostępne środowisko wirtualne. IoCT, jak nazywana jest ta dziedzina, będzie zapewne potrafiła wysoko waloryzować i wzbogacać, także upowszechniać obiekty kultury, także uzyskując ze swojej działalności profity edukacyjne, społeczne i ekonomiczne. Mariaż IoT i kultury, bardzo szeroka i fascynująca dziedzina badawcza, niesie ze

sobą także wiele wyzwań technicznych i informacyjnych. Można wymienić takie jak: semantyczna reprezentacja wiedzy dotyczącej dziedzictwa kulturalnego, prezentacja świadoma odbiorcy, nowe techniki multimedialne, techniki 3D i immersyjne, poszukiwanie wiedzy i opinii w mediach społecznościowych, nowe techniki Big Data dla informacji kontekstowych, modelowanie i naukowe odtwarzanie historyczne, wiele technik e-lerningu dla edukacji, dokumentacji i szkolenia, kształcenia, upowszechniania i popularyzacji w obszarze dziedzictwa kulturalnego, itp. Można i trzeba byłoby na ten temat fascynujący napisać znacznie więcej, ale zgodnie z regułami niniejszego opracowania, tylko sygnalizujemy tematykę. Jeśli ktoś ma wątpliwości jak fascynujący i przyszłościowy jest to temat, i jednocześnie obszar edukacyjnego IoT, to uprzejmie polecam wybranie się do polskiej stolicy ceramiki Opoczna i tamtejszego Muzeum Zamkowego. Sfinansowany przez UE projekt wirtualizacji historii miasta jest pewnego rodzaju wzorem co może być zrobione w tym obszarze. Ciekawa historyczna wizualizacja przez wieki w sposób interaktywny pokazuje np. że układ wielu ulic w tym samym, ale nie takim samym mieście jest taki sam jak prawie przed tysiącem lat. Statyczne obiekty dziedzictwa historycznego zostały pokazane dynamicznie, multimedialnie, i co więcej w sposób bardzo ciekawy. Takich wizualizacji, nawet o charakterze immersyjnym, jest znacznie więcej, np. dotyczących okresu przedpiastowskiego i wczesnopiastowskiego z okolic Gniezna i Kalisza.

Oddziaływanie IoT na człowieka jest znacznie bardziej skomplikowane niż opisano wyrywkowo powyżej dla kilku wybranych obszarów jego działalności. Trzeba jednak te rozważania kiedyś zakończyć, kontynuując je gdzieś indziej, i przejść do krótkiego opisu wybranych, i zapewne mniej ciekawych dla szerszego grona czytelników, procesów transformacji technicznej. Procesy te pokazują, gdy obserwuje się je z bliska, z dostatecznie niewielkiej odległości pozwalającej na zrozumienie i wniknięcie w niektóre szczegóły technologiczne, masywność zachodzącej transformacji. To co dzieje się na rynku i jest obserwowalne dla przeciętnego konsumenta jest jedynie wierzchołkiem góry lodowej. Pod powierzchnią trwa wielka przemiana, wielka integracja i konwergencja wielu dojrzałych technologii na być może wspólną, kiedyś być może jednolitą, inteligentną, cyfrową, informacyjną, wysoce funkcjonalną platformę cywilizacyjną.

Procesy transformacji IoT, RIoT, CIoT, IoT^{C} i IIoT

Technologie analogiczne do tego co nazywamy dzisiaj IoT były stosowane w nauce dużo wcześniej niż ten termin został użyty pierwszy raz i następnie, jak obserwujemy, zadomowił się na dobre. Mówimy o takich technologiach jak np.: zastosowania inteligentnych sieci czujnikowych, podejmowanie decyzji wspomaganych statycznymi i dynamicznymi danymi oraz inteligencją obliczeniową, ekstrakcja informacji i następnie wiedzy z danych masowych, usieciowienie i monitoring dużych zasobów sprzętowych, predykcyjne utrzymanie infrastruktury, modelowanie i mapowanie infrastruktur badawczych, geograficzne bazy danych sprzętu i całych eksperymentów. Nauka jest jednym z najbardziej intensywnych obszarów rozwoju i zastosowania IoT. Duże eksperymenty badawcze stosują czasami nawet setki milionów kanałów obserwacyjnych z czujnikami wielu mierzonych wartości fizycznych. Tak jest np. w eksperymencie LHC w CERN. Nauka stosuje w tych systemach, niespotykane w innych obszarach dokładności działania systemów IoT w sensie rozdzielczości czasowej, przestrzennej, spektralnej, energetycznej, polaryzacyjnej, fazowej, itp. Takie nasycenie technologii IoT jest nie spotkane gdzieś indziej. Takich wielkich eksperymentów w sali świata jednak nie jest dużo, może kilkaset, fizycznych, chemicznych, kosmicznych, medycznych. Badawcze i pilotowe rozwiązania nie są masowe. Nauka proponuje rozwiązania, czasami wskazuje kierunki, często błądzi, ale o dalszym rozwoju raczej nie decyduje. Potencjalna akceptacja i ewentualnie masowość aplikacji to są atrybuty wyłącznie rynku konsumenckiego zarządzanego często emocjami, także militarnego zarządzanego jeszcze innymi powodami.

Procesy transformacji IoT od nauki do przemysłu odbywają się w wielu różnych obszarach, na wielu różnych płaszczyznach technicznych i nietechnicznych, społecznych i ekonomicznych. Można wyodrębnić kilka cech charakterystycznych takich procesów prowadzących do umożliwienia i przyspieszania transformacji. Wymieniamy poniżej raczej czynniki pozytywne.

– Szybsza transformacja w obszarach IoT intensywnych, np. w sporcie, medycynie, biznesie ICT, niektórych działach przemysłu energetyce, technologiach kosmicznych,;

– Konwergencja różnych zaawansowanych technologii ICT i innych z IoT np. SCADA, HART, GIS, itp.;

– Lawinowy rozwój aplikacji amatorskich wspomagany dostępnością, znaczną rozmaitością i niewielkim kosztem komponentów IoT;

– Bogactwo rynku konsumenckiego i relatywna łatwość, oraz co ważniejsze opłacalność ekonomiczna transformacji produktów;

– Bogactwo dostępnych technologii bezpośrednich i skorelowanych z IoT i możliwość przejścia ewolucyjnego;

– Powszechne i urozmaicone wsparcie społecznościowe dla procesów transformacji;

– Poważne zaangażowanie badawcze i rozwojowe, finansowe i logistyczne wielu rządów, konsorcjów naukowo-przemysłowych i gigantów technologicznych w procesy transformacji;

Wśród czynników trudniejszych można wymienić znaczne koszty transformacji w dużej skali przemysłowej, i to wtedy jeśli dokonywane są nie ewolucyjnie a przez wymianę sprzętu na nową generację. Duże organizacje przemysłowe mogą sobie na to pozwolić np. w przemyśle motoryzacyjnym, lotniczym, energetyce, górnictwie, wymieniając całe linie produkcyjne.

Nie ma możliwości objęcia w miarę całościowo tych procesów w krótkim opracowaniu. Ograniczamy się do przyglądnięcia się niektórym, subiektywnie wybranym elementom składającym się na szerokie procesy przemian. Niepełnego wyboru dokonano jednak tak, aby zarysować jak najbardziej prawdziwy obraz zachodzących zmian i ich wpływu na naszą najbliższą przyszłość. Najbliżej człowieka są urządzenia użytkowe i one doznają obecnie szybkiej przemiany w wersje usieciowione czyli w elementy systemu IoT. Aktualne oceny rozwoju rynku urządzeń użytkowych, wykonywane okresowo przez firmy analityczne i inwestycyjne, także przez agencje rządowe, np. International Trade Administration, BI Intelligence, Tractrica, Gartner, Postscapes, IHS Markit, IDTechEx, CloudTweaks, i inne, wskazują, że IoT podąża do zajęcia w tym sektorze przemysłu i handlu pierwszego miejsca. Głównymi inwestorami obecnie w rozwój rynku przemysłowego IoT, o miliardowym poziomie inwestycji są następujące firmy, wg. kolejności: Intel Capital, Qualcomm Ventures, Foundry Group, KPCB – Kleiner Perkins Caufield & Byers, Andreessen Horowitz, Khosla Ventures, True Ventures, Cisco Investments, NEA – New Enterprise Associates, Sequoia Capital, First Round Capital, SVAngel, Crunch Fund, Felicis Ventures. Wśród setek najaktywniejszych firm typu start-up wspieranych przez inwestorów globalnych i produkujących dla sektora IoT wymieniane są np.: 3DR – 3D Robotics, Whistle Lab, AeroScout, AirWare, BodyLabs, Bocom INT, Jawbone, Leap Motion, Fitbit, mCube, Kinsa, Lockitron, CellScope, littelBits, Olio Cevices, Misfit, Sano Intelligence, iControl Networks, goTenna, ivee, AliveCor, Orbotix, Senseonix, Motiv, MarkerBot, Relayr, Revolv, Telogis, smart-FOA, Grid Net, FreedomPop, Performance Lab, MetroMile, Placemeter, Streetline, Quanttus, Quirky, Veniam, Sifteo, Impinj, JouleX, Yuneec, Waze, Sotera, Verdiem, Wearable Intelligence, Worldsensing, Skycatch, SigFox, Stratoscale, Panoramic Power, Skully Helmets, Topera Medical, Revolar, i inne. Fundusze kapitałowe wielkich firm technologicznych inwestują głównie w rozwój czujników, elektroniki ubieralnej, i zastosowania medyczne, także drony, a więc w brzegowy obszar IoT. Nic w tym dziwnego, ten obszar IoT jest bezpośrednim klientem masowo produkowanych przez te firmy mikroprocesorów. Setki znakomitych pomysłów na rozwój IoT można znaleźć samodzielnie na portalach crowdfundingowych jak Kickstarter, Indiegogo, FundRazr, MicroVentures, i innych podobnych. Są tam także pomysły z Polski. Wiele z tych pomysłów znalazło stosowne początkowe finasowanie realizacyjne. Kluczem na dzisiaj jest akceptacja użytkownika. Kluczem na jutro jest zwiększająca się szybkość uczenia rynku, co zapewne zwiększy elastyczność wprowadzania różnych aplikacji IoT.

Nauka i przemysł, IoT a szczególnie RIoT i IIoT, są od zawsze, także jeszcze obecnie kategoriami wzajemnie dość odległymi pod względem technicznym, logistycznym, aplikacyjnym, potrzeb, stopnia zrozumienia i odbioru społecznego, poziomu stosowanych technologii, finalnych produktów, bieżących potrzeb, polityki i ekonomii, zupełnie inaczej dążące i rozliczane z sukcesu, itp. W przyszłości mamy nadzieję, że także za sprawą IoT, odległość nauka – przemysł będzie malała. Nauka tworzy nowe koncepcje, modele, analizuje, testuje pojęcia i nowe rozwiązania, sprawdza możliwości wykorzystania teorii. Przemysł tworzy wartości fizyczne w postaci urządzań o poziomie konsumenckim. Dwa odmienne światy, słabo przystające do siebie, które jednak muszą tworzyć małżeństwo z rozsądku. To małżeństwo jest rozgrywane inaczej w różnych regionach globu, w różnych krajach. W pewnych miejscach znacznie sprawniej niż gdzieś indziej. Różnica jest łatwo obserwowalna przez każdego. Mówimy tylko o naukach stosowanych, technicznych, ale także chemicznych, fizycznych, biologicznych, medycznych, rolniczych i innych, których

zainteresowaniem są wyniki potencjalnie aplikowane. A mimo to nadal dystans nauka stosowana – przemysł jest znaczny. Sama nauka zmienia się pod wpływem IoT. Udostępnia w otwarty sposób surowe dane naukowe eksperymentów w chmurach instytucjonalnych jak CERN, lub indywidualnych jak w systemie Mendeley. Kiedyś to było nie do pomyślenia. Inżynieria materiałowa pracuje nad materiałami, potencjalnie funkcjonalnymi, które zostaną być może zastosowane w przemyśle za wiele lat. Technologia elektronowa pracuje wyprzedzająco nad układami elektronicznymi o charakterystycznym wymiarze poniżej 1 nm. Szerokie aplikacje praktyczne takich rozwiązań będą wg. oceny specjalistów nie wcześniej niż za kilkanaście lat. Wielu specjalistów z różnych dziedzin pracuje nad komputerem kwantowym, nad biosensorami, których szerokich zastosowań nie oczekuje się jutro. Teleinformatyka pracuje nad wirtualizacją wszystkiego, sieci, użytkowników, źródeł energii, rzeczywistości, programistyczną definicją sieci SDN i ich użytkowników. Te prace jeszcze długo będą kontynuowane w kierunku stworzenia konkretnych przydatnych usług. W wielu laboratoriach na świecie trwają intensywne prace nad bateriami. Jedną z koncepcji jest zastosowanie technologii tajwańskiego instytutu ITRI baterii typu URA – Ultrafast Rechargeable Aluminum zawierającej Al i grafit. ITRI pracuje również nad wieloma innymi rozwiązaniami dla IoT jak: e-papierem, nową generacją plazmonowych organicznych diod elektroluminescencyjnych pcoLED, ortozy z rozłożonymi i precyzyjnymi czujnikami zbliżenia i dotyku. Takich przykładów można podać bardzo wiele, praktycznie w każdej dyscyplinie i specjalności naukowej, telematyce, optyce, mechatronice, mikrofluidyce, informatyce, automatyce, robotyce, multimediach i technikach informacyjnych, i wielu innych. Wiele z tych rozwiązań trafi na rynek, ale nie wszystkie i nie natychmiast.

Transformacja IoT – IIoT wymaga pokonania kilku barier technicznych i pozatechnicznych. W światowej literaturze przedmiotu IoT mówi się o procesie 4C – cloud- culture-clash-change, chmura-kultura-zderzenie-zmiana, podkreślając tym że technologia IoT i chmury nie jest zmianą ilościową a istotną zmianą jakościową, prowadzącą często przez konflikt do zmiany kultury biznesowej. Zastany przemysł wytwórczy istnieje od pewnego czasu, od dawna, używa rozwiązań sprawdzonych zaprojektowanych jakiś czas temu, przeznaczonych do funkcjonowania przez dłuższy okres czasu, zaprojektowanych często do produkcji masowej. Sygnały używane do obsługi wielu działających urządzań przemysłowych to często setki V i znaczne prądy. Automatyka bazuje na typowych powszechnie używanych rozwiązaniach przemysłowych, spełniających dobrze sprawdzone normy. Przemysł wytwórczy nie jest transformowalny z dnia na dzień. Transformacja linii produkcyjnej jest planowana ze sporym wyprzedzeniem i jest bardzo kosztowna. A jeszcze jeśli linia działa sprawnie i robi na razie to co trzeba, to ochota właścicieli na szybką transformację jest niewielka. Wszystko to, warunki pracy, sygnały, standardy, jest zupełnie niekompatybilne z nową generacją sprzętu IoT gdzie prądy i napięcia to pojedyncze V i mA. Płyty systemowe obsługujące urządzania IoT, np. takie jak niezwykle popularna w rozwiązaniach IoT Respberry PI, są zupełnie nie odporne na przemysłowe warunki pracy, chyba że umieści się je w chronionych szafach przemysłowych i dodatkowo zabezpieczy sygnałowo i pod względem EMI – interferencji elektromagnetycznej. W skrócie można powiedzieć, że obecnie główną rolą transformacji IoT w IIoT w wielu przypadkach działającego dostatecznie sprawnie przemysłu wytwórczego jest danie nowego życia starym urządzeniom, najpierw odmłodzenie a dopiero w następnej kolejności ewentualna przemiana pokoleniowa. Szczególnymi obszarami IIoT rozwijanymi w pierwszej fazie modernizacyjnej w ustabilizowanym przemyśle wytwórczym jest usieciowienie urządzań i maszyn i na tej podstawie dodawanie nowych funkcjonalności związanych z wydajnością procesów wytwórczych, zwiększeniem jakości produkcji, poprawą niezawodności, zastosowaniem diagnostyki predykcyjnej, obniżeniem kosztów, itp. Zupełnie odmienna sytuacja jest w przemyśle i biznesie informacyjnym, informatyce, usługach, małych i średnich firmach innowacyjnych jednoproduktowych lub kilkuproduktowych. Tutaj przemiany można dokonać niemal natychmiast, i tak się właśnie robi. IoT bez wątpienia transformuje przemysł. Wywiera na niego coraz większą presję. Podane przykłady realnych obecnie działających zastosowań elementów systemu IoT w przemyśle wyglądają na pierwszy ogląd trywialnie w porównaniu z tym nad czym pracuje nauka. Tak jednak nie jest. Każde a tych rozwiązań niesie w sobie pewien istotny element innowacyjności. Stoją za tym także koszty i czasami znaczny wysiłek przemiany mentalnej. Z tych niewielkich cegiełek, integrowanych pieczołowicie w większe systemy już niedługo będą budowane nowej generacji sprawne systemy przemysłowe. Zacznijmy w opisie niektórych obszarów przemysłowych zastosowań IoT od czegoś już realizowanego dzisiaj, bliskiego realizacji jutro w zakresie mniejszych i większych systemów autonomizowanych i podążajmy w przyszłość.

Jeśli trzeba byłoby wymienić pojedynczy sprzętowy element strategiczny od którego zależy cały rozwój obszaru brzegowego IoT to bez wątpienia jest to mikrokontroler, a wcale nie różne rodziny czujników i aktuatorów. Obecnie w najnowszym rozwiązaniu mikrokontroler jest określany terminem „system na układzie scalonym" i skrótem SoC. Jest to pojedynczy mikroukład scalony posiadający pełną funkcjonalność komputera stosowanego w zastosowaniach wbudowanych. Jaki musi być układ SoC dla IoT? Powinien umożliwiać wielokanałową integrację z urządzaniami brzegowymi, czyli musi być niezawodny, mały i tani (Pfister 2011), (Kuhnel 2015). Wymiarowo nie powinien przekraczać 1 lub najwyżej kilka mm^2 dla zastosowań w najbardziej popularnych węzłach końcowych sieci wyznaczających jej brzeg, oraz poniżej 1 mm^2 w inteligentnych mikro-czujnikach, w cenie najlepiej poniżej 1 $ i pobierać moc znacznie mniejszą niż 1 mW. Powinien dysponować wielokrotną magistralą CAN, dostatecznymi zasobami pamięci, licznymi portami I/O, i posiadać urozmaicone środowisko programistyczne i bezpieczeństwa, np. wbudowane w SoC klasy ARM TrustZone CryptoCell. Intel zaprezentował pod koniec 2016 r. nową wersję SoC Atom o możliwościach działania w czasie rzeczywistym, przeznaczoną do zastosowań w przemyśle motoryzacyjnym. Dla węzłów końcowych i mikroczujników IoT Intel odnawia różne serie mikrokontrolerów Quark x86. ARM, obok firm Renesans, NXP, i Mikrochip, jest zdecydowanym liderem w produkcji mikrokontrolerów Cortex-M dla węzłów końcowych sieci IoT i mikroczujników. Do tej pory, przed początkiem masywnych zastosowań układów SoC w IoT, środowisko aplikacyjne systemów wbudowanych nie rozwijało specjalnie technologii bezpieczeństwa. Teraz, w pewnym sensie, trzeba ten brak nadrobić. ARM TrustZone dla procesorów Cortex-M idzie w tym kierunku. W budowie systemu IoT powyżej pojedynczego mikrokontrolera jest gotowy moduł aplikacyjny składający się z układu scalonego, systemu operacyjnego w tzw. postaci wbudowanej, pamięci, układu zasilania lub pobierania energii ze środowiska, interfejsów wejściowo wyjściwych I/O do współpracy z czujnikami, aktuatorami – elementami wykonawczymi i liniami transmisyjnymi. Do budowy zaawansowanych interfejsów IoT stosowanych jest wiele dostępnych obecnie komercyjnych, przyjaznych dla użytkownika, tanich, niskoenergetycznych i miniaturowych rozwiązań z systemami wbudowanymi np. właśnie z wykorzystaniem procesora ARM Cortex i systemu operacyjnego mbed. Takie układy jednomodułowe ze środowiskiem programistycznym, np. PICO-IMX6 Aries embedded, Xilinx Zynq Ultra Scale MPSoC, Vivado HLS, Altera Stratix SoC IoT modules, Telit LTE modules, SIERRA Wireless, Toradex –Calibri T30, Iris CB, Satori IoT Dev Tool, Infineon, Arrow Electronics, i wiele innych, posiadają znaczne zasoby obliczeniowe i mogą stanowić silne węzły brzegowe IoT. Są dostępne w wersjach prostych tanich ale i bardzo zaawansowanych, ze znormalizowanym środowiskiem do łatwego i szybkiego prototypowania sprzętu i oprogramowania SDK i HDK – software and hardware development kits. Coraz częściej sprzedawanych pod komercyjnymi nazwami IoT Kit dla Androida ale i dla Windows. Środowisko prototypowania rozwiązań IoT zawiera platformę rdzeniową oraz bazę danych komponentów. ARM proponuje dla rozwiązań IoT subsystem wbudowany CoreLink SSE-100 współpracujący z inteligentnym systemem radiowym Bluetooth Cordio, usługami w chmurze, systemem operacyjnym mbed i procesorem Cortex-M, a także środowiskiem programistycznym Cadence Hosted Design Solutions – dostępnym jako usługa typu SaaS – Software as a Service, będącym jednym z modeli chmury obliczeniowej. Rozwój szerokiej grupy usług zewnętrznych typu cloud computing: SaaS, IaaS – infrastructure as a service, oraz PaaS – platform as a service, ale także C-IoT cloud based innovative and collaborative IoT jest obecnie integrowany i podlega ewolucyjnej konwergencji w IoT (cloudcomputing.pl), podobnie do wielu innych wymienionych poprzednio technologii sprzętowych, programistycznych i usług. Przykładowo dwumodułowy, pełny sprzętowo programistyczny zestaw projektowy IoT dla 'początkujących' Toradex zawiera płytki prototypowania Colibri, Iris CB z układami ARM Cortex, Nvidia Tegra, pamięciami DDR i eMMC, interfejsami I/O USB, OTG i Eth. Oprogramowanie jest wykonywane pod systemem operacyjnym Windows korzystając ze środowiska VS Visual Studio oraz Azure IoT Suite. Potencjalną konkurencję dla układu Raspberry Pi, który świętował niedawno sprzedaż kilkunastu milionów egzemplarzy, stanowi zorientowany na IoT PC jednopłytkowy o większych zasobach obliczeniowych Hikey 960. Układ jest firmowany przez Google i Huawei. W projekcie tego układu brały udział dodatkowo, oprócz wymienionych, takie firmy jak ARM, Archemind oraz

LeMaker. Ten bardzo uniwersalny układ do budowy silnych węzłów IoT bazuje na procesorze SoC HiSilicon Kirin 960 stosowanym w topowym smartfonie Huawei P10. Zastosowano pamięć wspomagającą 3 GB RAM LPDDR4 i masową 32/64 GB. Obsługę danych obrazowych aż do rozdzielczości 4K zapewnia procesor GPU ARM Mali G71. Obecne złącze HDMI ver. 1.2. obsługujące tylko rozdzielczość FHD będzie wymienione na wyższą generację 1.4 lub 2.0. Układ posiada złącze M.2, wielopinowe złącza I/O, dwuzakresowy port Wi-Fi i obsługuje standardy komunikacyjne 802.11ac oraz Bluetooth 4.1. Całość jest obsługiwana przyjaźnie dla użytkownika z poziomu systemu operacyjnego Android 7.1 Nougat.

O sprawności konwersji IoT w dużej mierze decyduje dzisiaj dostępność tanich, wstępnie oprogramowanych modułów szybkiego prototypowania z wbudowanym systemem operacyjnym, a także środowisk programistycznych i platform ekosystemowych. Niektóre przykłady takich funkcjonalności wymieniono powyżej. Moduły do szybkiego prototypowania IoT są ogólnego stosowania, a także częściowo lub całkowicie specjalizowane dla konkretnego sektora biznesu, usług, przemysłu wytwórczego, także rynku konsumenckiego (Faihead 2016), (Guinard 2016), (Shovic 2016), (Rogers 2017). Specjalizacje dotyczą w szczególności dużych obszarów konwergencji lub zastosowań IoT jak: GIS – geograficznych systemów informacyjnych, czyli geodezji i kartografii, przemysłów – samochodowego, lotniczego, transportu, kosmicznego, energetycznego, handlu, itp. Przeglądnijmy w skrócie niektóre parametry i funkcjonalności jeszcze kilku innych wybranych układów szybkiego prototypowania IoT, a w szczególności układów otwartego sprzętu i oprogramowania. Otwarty źródłowo moduł panSTamp NRG2 jest zbudowany na SoC CC430, zawiera rdzeń układu mikrokontrolera MSP430, oraz moduł radiowy ultra niskiej mocy TI CC1101, a także trzyosiowy akcelerometr i zintegrowany czujnik temperatury i wilgotności. Moduł bazowy panSTamp AVR2 jest zbudowany na popularnym mikrokontrolerze Atmega328p i radiowym układzie I/O CC1101. Bardzo oszczędny energetycznie układ radiowy, stosując protokół M2M, pracuje w otwartym pasmie 868-915 MHz i może działać kilka lat na jednej baterii alkalicznej, zapewniając łączność na odległość kilkaset metrów a nawet do kilku kilometrów w otwartej przestrzeni. Transfer standardu komunikacyjnego M2M do IP jest dokonywany w wirtualnym mostku sieciowym używając makra sieci web lub własne skrypty klienta napisane w języku Python. Do czego są zdolne tak trywialnie proste rozwiązania modułowe i jak szerokie mogą być ich zastosowania, dzisiaj na początkowym etapie rozwoju IoT? Zamiast rozwijać własny produkt od początku, dostępne biblioteki funkcjonalne panSTamp i wbudowane protokoły komunikacyjne pozwalają na przyspieszone prototypowanie swojej aplikacji poprzez skupienie się tylko na niej i rozwój wyłącznie jej funkcjonalności charakterystycznych. Używając wymienionych modułów można stworzyć pełen bezprzewodowy ekosystem funkcjonalny IoT podłączony prostą bramką do lokalnej sieci IP. Wątpliwości aplikacyjne i wspomaganie projektów funkcjonalności IoT jest dostępne na przyjaznym forum panstamp.org. W analogiczny sposób, jak podano w powyższym przykładzie, działa wiele społecznościowych środowisk używających systemy jedno i wielomodułowe, dostępnych jako otwarte komercyjnie bądź w postaci otwartych bibliotek projektów sprzętu i oprogramowania. Fora społecznościowe panSTamp, Arduino, Piko, ARM, Atmega, MTCA, itp. prowadzą dokumentację raportowania błędów nowego sprzętu i oprogramowania, udostępniają wyniki beta-testów sprzętu i oprogramowania, oraz całych aplikacji, komentują nowe kierunki rozwoju, odpowiadają na proste i skomplikowane pytania konstruktorów aplikacji IoT, itp.

Innym przykładem odmiennego, ortogonalnego ale silnie uzupełniającego do poprzednich, działania w obszarze IoT są dostawcy pełnych, gotowych, zintegrowanych platform funkcjonalnych IoT, nazywanych platformą IoT, ekosytemem IoT lub aktywatorem IoT. Takie platformy łączą typowo technologie chmura/IoT/M2M oraz SaaS. Odmienne, bardziej konserwatywne produkty integracyjne IoT są dostępne u większych dostawców. Wśród dostawców innowacyjnych, a na ogół są to relatywnie niewielkie firmy, choć także są i więksi gracze dostarczający rozwiązań całościowych typu end-to-end, można wymienić np. Telit, Cumulocity, Carriots, ThingWorx, Ayla, EuroTech, Relayr, EMnify i inne. Takie firmy specjalizują się na ogół w IoT-yzacji ściśle wybranych sektorów dużego przemysłu np. petrochemicznego, transportu, farmaceutycznego, chemicznego, handlu, ipt. Niektóre wręcz przeciwnie specjalizują się we współpracy z innymi niewielkimi firmami innowacyjnymi w sektorach IoT intensywnych. Wśród przykładów dostępnych ekosystemów wdrożonych praktycznie można wymienić np.: zarządzanie dystrybucją leków rozprowadzanych w miniaturowych mobilnych lodówkach (definitiv), zorientowane na potrzeby klienta zarządzanie aplikacjami i urządzeniami (T-mobile), automatyzację łańcucha dostaw dla dystrybutorów konsumenckich i przemysłowych (Lyreco), śledzenie pojazdów i analityka rolnicza (STW), masowa sieć M2M/IoT dla przedsiębiorstw (T-mobile), zarządzanie rynkiem konsumenckim (MicroTechnology CUMoNoSU), zarządzanie monitoringiem i serwisowanie urządzeń przemysłowych (Gardner Denver), analityka w czasie rzeczywistym i predykcyjne utrzymanie sprzętu (Certus), zintegrowane usługi online dla produktów konsumenckich (Trackerando) i przemysłowych (Telit), i wiele innych.

Znaczną siłę przyciągania dla producentów nowoczesnego IoT-yzowanego sprzętu konsumenckiego, twórców standardów dla tego sprzętu w tym standardów komunikacyjnych posiada nasz dom. Nasze mieszkanie, nasz dom, biuro, bezpośrednie otoczenie dłuższego przebywania człowieka jest bardzo atrakcyjnym miejscem potencjalnej silnej i szybkiej penetracji przez IoT. Ten teren jest także potencjalnie IoT intensywny. Przykładem jest kolejny proces konwergencji zastanych technologii stosowanych obecnie powszechnie w domu w kierunku IoT. Za standaryzacją takich procesów konwergencji stoją także interesariusze przemysłowi i społecznościowi. Fundacja OCF – Open Connectivity (openconnectivity.org), Konsorcjum DLNA – digital living network Alliance (dlna.org), duże przemysłowe firmy sieciowe, sprzętu konsumenckiego, AGD, jak np. Belden, Samsung, Electrolux, Whirlpool, i inne.Standard rozpowszechniania mediów w sieci domowej DLNA/UPnP stanowi bardzo dobrą zastaną infrastrukturę do konwergencji. DLNA posiada same zalety z punktu widzenia użytkownika. Nie wymaga praktycznie żadnej konfiguracji. Wymagany jest prosty serwer DLNA którym może być PC z aplikacją, telewizor, dysk sieciowy ze wsparciem DLNA, oraz klienci DLNA. Jednym z projektów konwergencji technologii przemysłowych i konsumenckich sponsorowanych przez OCF jest IoTivity (iotivity.org). Celem działania OCF i projektu IoTivity jest prowadzenie działań w zakresie unifikacji podobnych protokołów komunikacyjnych sprzętu i usług w grupy funkcjonalne i objęcie ich standardem IoT. Oprócz DLNA do komunikacji multimediów domowych są stosowane protokoły i systemy własnościowe: AirPlay, Miracast, NAS, Cloud Storage. Unifikacja tego atrakcyjnego komercyjnie obszaru, i konwergencja pod parasolem IoT jest logicznym kierunkiem rozwoju.

Rozwijana technologia sieci komunikacji mobilnej 5G, będąca następcą 4G/LTE jest konieczna dla rozwoju IoT i IIoT i ich transformacji w powszechne środowisko infrastrukturalne. Czasami generacja 5G nazywana jest jako podstawa funkcjonalna IoT w ogóle, nie tylko bezprzewodowego (Markakis 2017), (Mavromoustakis 2016). Jako potencjalną datę rozpoczęcia wprowadzania technologii 5G w sensie dostępności dla użytkownika podaje się obecnie rok 2025. Koszt oceniany jest na setki miliardów Euro. Czym te technologie 4G i 5G różnią się zasadniczo od siebie. Po pierwsze, kilkudziesięciokrotnym wzrostem nominalnych prędkości transmisji danych. Tylko taka różnica byłaby jednak nie warta wprowadzania aż zmiany numeru generacji. Po drugie i najważniejsze, kompletną zmianą filozofii myślenia o wykorzystaniu pasma transmisyjnego. Obecnie wykorzystanie pasma jest katastrofalnie nieefektywne i wynosi w najlepszych przypadkach zaledwie kilkanaście procent, nawet w centrach wielkich miast. Wynika to z tradycji stałego przyznawania części pasma wielu ważnym instytucjom. Tak ważnym, że nie wiadomo które ważniejsze, jak: obronność i bezpieczeństwo czyli wojsko i policja, straż pożarna, służby, komunikacja i transport, usługi, handel, biznes, zdrowie, radio i telewizja, rząd, administracja centralna i lokalna, samorządy, i wiele innych. System 5G odchodzi, choć jeszcze tylko częściowo, od sztywnego podziału pasma. Ale i tak wykorzystanie ma się zwiększyć do kilkudziesięciu procent. W dalszej przyszłości czeka nas pełna elastyczność przyznawania pasma, całkowite współdzielenie zasobów, i kompletna wirtualizacja infrastruktury. Mówiąc nieco żartobliwie, także zdrowie i bezpieczeństwo stanie się usługą, a przede wszystkim kognitywna stanie się mobilność. Mówiąc bardziej technicznie, użytkownikami sieci 5G będą np. kognitywne radio i multimedia, kognitywna robotyka, usługi, itp. Standaryzacja systemu 5G dopiero się rozpoczyna i uczestniczą w niej, między innymi, takie instytucje i firmy jak IEEE, Samsung, Huawei, Nokia, Qualcomm, NGMN Alliance – Next Generation Mobile Networks, ITU, i inne. Powstają początkowe projekty sprzętu 5G, takie jak np. modem Snapdragon X50 5G pracujący obecnie w paśmie milimetrowym 28 GHz, a w przyszłości w nowej wersji do 90 GHz, umożliwiający transmisję danych z prędkością ok. 40 Gbps w paśmie nie przekraczającym 1 GHz. Zwiększona efektywność wykorzystania pasma pozwala na gęstsze upakowanie szerokopasmowych użytkowników IoT oraz na znaczne zwiększenie niezawodności masywnej komunikacji M2M. Dalsze konsekwencje

wprowadzenia technologii 5G to zmniejszenie latencji do poziomu nawet sub-milisekundowego, mniejsze zapotrzebowanie na energię, w tym zwiększenie efektywności energetycznej transmisji, inteligentne zarządzanie przepustowością, masowe zastosowanie technologii Li-Fi światła widzialnego i podczerwonego z DEL oświetleniowych do lokalnej transmisji danych, tworzenie dynamicznych ad-hoc sieci kognitywnych w odpowiedzi na lokalne zapotrzebowanie, standaryzacja platformy transportowej, budowa systemu zorientowanego na użytkownika a nie operator-centrycznego, potencjalnie obsługa setek miliardów i więcej użytkowników IoT, inaczej mówiąc, w pewnym sensie, stworzenie bezprzewodowego świata bez limitu dostępu.

Czasami ten świat jest określany terminem WWWW – wireless WWW. Czy taki otwarty świat bezprzewodowy będzie odporny na epidemie i pandemie? Powoli zaczynają się pojawiać nowe zjawiska, potencjalne składowe przyszłych szerszych procesów, które w przyszłości mogą złożyć się na zagrożenie globalne. Jednym z takich zjawisk, wyrosłym z poprzednich dość dużych doświadczeń w bogatym obszarze działań złośliwych i szkodliwych, jest spamowanie i hakowanie IoT. To pierwsze polega, bardzo ogólnie mówiąc, na blokowaniu działania pojedynczych kluczowych urządzeń lub całych sektorów sieci brzegowej IoT poprzez generowanie niepotrzebnego lub fałszywego ruchu danych w odpowiednim otoczeniu sieciowym. To drugie jest nam także znane od dłuższego czasu i polega na przejęciu kontroli nad nie swoją własnością, a więc jest działaniem kryminalnym. Sieć globalna i świat bezprzewodowy ułatwia takie działania. Nie ma co liczyć na to że takie działania nie będą podejmowane wobec IoT, napędzane mechanizmami biznesowymi, ekonomicznymi i politycznymi. A jeśli takie możliwe zjawiska potrafimy przewidzieć już dzisiaj, to oznacza że IoT jest lub kiedyś będzie potencjalnie narzędziem, i szerzej potężnym zjawiskiem, ekonomicznym, politycznym i społecznym. Powtarzamy tutaj tą groźnie brzmiącą tezę – ostrzeżenie wielokrotnie, prawie do znudzenia, ale jeśli powtarza ją szeroko światowe, naukowo – techniczne środowisko badawcze to oznacza to zupełnie coś innego niż następujące potem, potwierdzone stosownymi badaniami, tezy środowisk socjologicznych i humanistycznych. Najgorzej będzie jeśli tezy zakorzenione w bardzo różnych światach badawczych będą stawać się kiedyś w jakiś sposób zbieżne. Poprzez swój potencjalnie globalny charakter w przyszłości, jeśli rzeczywiście rozwój pójdzie w kierunku globalizacji, a nie rozbicia dzielnicowego, IoT może stać się albo uniwersalnym panaceum na problemy gospodarcze świata, albo także następnym rodzajem broni masowego rażenia. Do tej pory ludzkość jakoś szczęśliwie utrzymywała taką broń w ryzach. Myślmy raczej o pozytywach, o wielkich korzyściach z istnienia kiedyś globalnej sieci IoT w postaci standaryzacji produktów i usług, znacznego ułatwienia działań gospodarczych, rozpowszechnienia pożytecznych usług w tym dotyczących ochrony zdrowia, znacznego obniżenia kosztów produkcji, wielkich oszczędności zasobów naturalnych i przyspieszonego, ale zrównoważonego rozwoju cywilizacyjnego.

Od strony sprzętowej fundamentem IoT jest mikroprocesor. Od strony programistycznej jest to wielowarstwowy protokół komunikacyjny, budujący funkcjonalności i inteligencję IoT. IoT korzysta zarówno z zastanych, dobrze ustabilizowanych, standardów telekomunikacyjnych (protokołów, znaczników, lokatorów, systemów nazw, systemów adresowania i pakowania zawartości, środowisk operacyjnych, itp.) np. zgodnych z powszechnie obowiązującym ogólnym, siedmio-warstwowym modelem odniesienia ISO/IEC ITU-T OSI – open systems interconnection reference model, jak i wypracowuje swoje. Najpowszechniej używany jest model uproszczony TCP/IP, który także zawiera w zasadzie wszystkie warstwy OSI ale grupuje je inaczej w cztery poziomy funkcjonalne, a więc w konsekwencji nie jest w pełni zgodny z OSI: aplikacji (aplikacji, prezentacji i sesji), transportu (część sesji i transportu), Internetu (sieci) i dostępu (łącze danych i fizyczna). Zagadnienie standardów komunikacyjnych, ścieżek transmisji sygnałów, protokołów, realizowanych usług, warstw oprogramowania sprzętu, ich różnicowania i subtelności jest fundamentalne dla burzliwego rozwoju IoT, jednak znowu możemy je omówić bardzo powierzchownie, wręcz jedynie zasygnalizować. Na drodze sygnału w Internecie i w systemie IoT napotykane są standardowe urządzenia sieciowe jak brama, router internetowy, mostek, wzmacniak/regenerator. Urządzenia te są związane z innymi warstwami modelu OSI, czy TCP/IP. Model sieci dotyczy prawie zawsze opisu ścieżki enkapsulowanych danych pomiędzy aplikacjami przez całą różnorodność sieci. A co się dzieje w przypadku kiedy aplikacja jest inteligentna i posiada swoją własną, czasami wielowarstwową, wewnętrzną strukturę? A tak właśnie się dzieje w przypadku IoT. Można opisywać sieć odrębnie w modelach klasycznych i aktywowany przedmiot IoT odrębnie np. behawioralnie, lub wyodrębniać dodatkowy poziom przedmiotowej czy brzegowej sieci proksymalnej i dostępowej. Można też próbować tworzyć nowe klasyfikacje warstw funkcjonalnych i inne modele specyficzne dla rozwijających się struktur IoT. Stąd biorą się właśnie próby zdefiniowania sieci IoT niejako od nowa, uwzględniając fundamentalną rolę inteligentnego obszaru brzegowego, jako potężnego źródła bardzo zróżnicowanych sygnałów i danych, korzystających z bardzo zróżnicowanych metod konwersji, transmisji, lokalnej akwizycji i dostępu. Jeśli jednak przyglądnąć się nowym warstwowym klasyfikacjom funkcjonalnym, to uwzględniają one w różnym stopniu pełne ujęcie klasyczne. Można pokusić się o zebranie i wymienienie tutaj niektórych z tak częściowo od nowa, a częściowo klasycznie, definiowanych technologii i protokołów transmisyjnych: infrastrukturalne, identyfikacyjne, komunikacyjno – transportowe, odkrywania sieci, protokoły danych, zarządzanie urządzeniami, semantyczne oraz wielowarstwowe ramy sieciowe. Te warstwy nie są jeszcze standaryzowane ale zyskują na popularności, są stosowane i widocznie lepiej oddają budowane i zmienne struktury sieci IoT, w tym sieć świadomą zawartości czy samoorganizujące się sieciowe struktury bezprzewodowe. Znakomity, bo wyczerpujący i przyjazny dla użytkownika, opis oprogramowania IoT można znaleźć na platformie postscapes. Środowiska IoT obejmują np. Thingworx, ioBridge, Sense i inne. Platforma opisuje i daje dostęp do protokołów, wbudowanych systemów operacyjnych, środowisk IoT, itp. Niektóre z protokołów IoT bardzo skrótowo przedstawiamy poniżej, zgrupowane funkcjonalnie.

Warstwa infrastrukturalna sieci IoT jest obsługiwana przez wiele technologii i specyficznych dla nich protokołów takich jak: PON – pasywna sieć optyczna, WDM, DWDM – gęste multipleksowanie kolorów, CWDM – przybliżone multipleksowanie kolorów, TDM – multipleksowanie w czasie, FTTx – światłowód do abonenta x, IPv4/IPv6 i jego odmiany i części składowe, mikro IP – µIP i nano-IP, UDP, QUIC – Quick UDP, Aeron – Unicast UDP, IPC, 6LoWPAN – bezprzewodowy 2,4 GHz protokół dla osobistej sieci IPv6 niskiej mocy – IEEE802.15.4, DTLS – datagramowa warstwa transportowa, ROLL – RPL/IPv6 – routowanie w sieciach niskiej mocy i stratnych, technologia TSMP – time synchronized mesh protocol odmiana TDM obsługuje bezprzewodowe sieci samoorganizujące się przedmiotów, najczęściej rozrzuconych czujników nazywanych pyłkami, technologia CCN – sieć dano-centryczna, inaczej świadoma zawartości przyszłej generacji. Sieć CCN, określana jako przyszłość IoT, routuje bezpośrednio do celu nazwane elementy zawartości na poziomie pakietowym. Taki sposób routowania wymaga znacznej nadmiarowości transmisji i jest mniej kosztowny w sieciach ultra szerokopasmowych. Jednak zawsze związany jest z tym większy koszt energetyczny. Z kolei sieć TSMP jest określana jako przyszły fundament budowy pewnych rodzajów obszarów brzegowych IoT, tych które będą zawierały bardzo wiele czujników np. monitorujących wielkie obszary środowiska naturalnego, takie jak rzeki wzdłuż ich całego kilkuset kilometrowego biegu. Inną charakterystykę posiada proces masywnego transportu danych świadomy aplikacji, sieci i kanału transmisyjnego. Identyfikuje on możliwości sieci i potrzeby komunikacyjne na podstawie informacji, przepływu, częstotliwości, dozwolonej latencji, wymaganego bezpieczeństwa, wymagań dotyczących wydajności energetycznej, określonej z punktu widzenia aplikacji, określa standard transmisji wymagającej np. potwierdzenia wiadomości czy jedynie dostarczenia typu best effort, deterministycznego, w czasie rzeczywistym czy programowanego.

Warstwa identyfikacyjna IoT jest obsługiwana przez takie standardy, znaczniki i protokoły, oraz formaty plików jak np. IPv6, URI, URL, URN, Postscript i EPS, µCODE, i inne. Warstwę komunikatów i transportu obsługują np.: LPWAN, BT, WiFi i wiele innych. Warstwę odkrywania sieci obsługują np.: UPnP, mDNS, HyperCat, Physical Web, i inne. UPnP – universal plug and play, o którym pisano poprzednio z okazji zastosowania w sieciach domowych, jest zestawem protokołów pozwalających na proste wzajemne odkrywanie się niektórych urządzeń w sieci. System nazw multicast mDNS przekształca w małych sieciach bez serwera DNS, a więc typowo dla małych węzłów brzegowych IoT, nazwy własne w internetowe adresy IP. HyperCat jest formatem prostego katalogu hipermedialnego bazującego na prostym formacie wymiany danych JSON – JavaScript object notation (json.org) niezależnym od konkretnego języka. HyperCat eksponuje zbiory nazw URI. Fizyczna sieć Web umożliwia użytkownikowi dostęp do listy adresów URL, które są rozgłaszane przez obiekty w środowisku użytkownika niskoenergetyczną metodą Bluetooth low energy beacon – BLE.

Warstwa protokołów danych w sieci IoT jest obsługiwana przez chyba najbogatszy zestaw narzędzi. Część z tych narzędzi konkuruje ze sobą, w tym sensie że są popularnie stosowane, obsługują podobne funkcjonalności, nie wypracowały sobie dostatecznej przewagi aby zostać określone jako bezwzględnie panujące standardy. Przykładem takiej konkurencji może być układ popularnych protokołów MQTT i XMPP. MQTT – message queing telemetry transport umożliwia komunikację M2M z odległymi lokalizacjami, subskrypcję i publikowanie wiadomości w sposób bardzo oszczędny pasmowo. XMPP (Jabber) – extensible messaging and presence protocol, bazuje na języku XML, i umożliwia przesyłanie wiadomości oraz metadanych w czasie rzeczywistym. Wykorzystywany jest najpowszechniej w komunikatorach a może służyć także do okresowego pobierania wiadomości M2M. Odmiana MQTT-SN jest optymalizowana do obsługi M2M, sieci czujnikowych i aplikacji mobilnych. Mosquito jest brokerem MQTT o otwartym kodzie oprogramowania. IBM MessageSight jest skalowalnym, wysoce niezawodnym protokołem przesyłania komunikatów do obsługi znacznej liczby wydarzeń. Przeznaczony jest do zastosowań w przemyśle. Dostępny jest także na platformy Android i iOS. CoAP constrained application jest prostym protokołem multicast, spełniającym standard RESTful, o bardzo niewielkiej nadmiarowości obsługującym warstwę aplikacji w przypadku urządzeń IoT o bardzo ograniczonych zasobach i jest łatwo tłumaczonym do http w celu szybkiej integracji z WWW. SMCP jest wersją CoAP dla zastosowań wbudowanych. Niektóre z innych protokołów w tej grupie to: STOMP – prosty tekstowy protokół komunikatowy; XMPP – rozszerzalny protokół komunikatowy i obecności oraz jego wersja interoperacyjna XMPP-IoT; AMQP – zaawansowany protokół kolejkowania wiadomości; DDS – usługa dystrybucji danych dla RTOS; Mihini/M3DA – agentowy, mediatorowy komponent programistyczny pomiędzy serwerem M2Mi aplikacją uruchomioną w sieciowej bramce wbudowanej, optymalizuje użycie pasma; LLAP – lekki, tekstowy lokalny protokół automatyki; LWM2M – standard systemowy M2M obejmujący DTLS, CoAP i inne; SSI – prosty protokół komunikacyjny nazywany interfejsem czujnikowym; JMS – usługi komunikatowe Java; RESTful http; SOAP – protokół dostępowy prostych obiektów; i inne. Nie bez przyczyny wymieniamy niektóre protokoły warstwy danych, ponieważ w tym obszarze prowadzone są szerokie badania nad ich rozwojem i poszukiwania rozwiązań optymalizowanych do zastosowania.

Warstwa komunikacyjna i transportowa używa protokołów, standardów i topologii sieciowych takich jak Ethernet, WirelessHART, DigiMesh, IEEE.802, NFC, ANT, Bluetooth, Eddystone, ZigBee, EnOcean, WiMax, LPWAN, NB-IoT, LTE-MTC, EC-GSM-IoT, LoRaWAN, RPMA, GPRS/xG, i innych. Warstwa Semantyczna używa standaryzowanych narzędzi: IoTDB, SensorML, SSNO, języków skryptowych np. Wolfram, RAML język modelowania RESTful API, SENML – czujnikowy język znacznikowy, LsDL – język obiektowy XML dla urządzeń usługowych. Programistyczne i architektoniczne środowiska wielowarstwowe IoT korzystają z takich narzędzi jak: Alljoyn – budowa urządzeń i aplikacji odkrywających i komunikujących siebie; IoTvity, opisany poprzednio IEEE P2413, Thread/6LoWPAN, Środowisko aplikacyjne IPSO, Weave – platforma komunikacyjna dla urządzeń IoT; Telehash. Warstwa bezpieczeństwa używa wiele narzędzi standaryzowanych i rozwojowych jak np.: OTrP – otwarty protokół zaufania; X.509 – standard dla infrastruktury klucza publicznego PKI, część protokołu TLS – bezpieczeństwa wartwy transportowej.

Jedną z możliwych efektywnych ścieżek transformacji przemysłowej IoT/IIoT jest ewolucyjna konwersja szeroko używanego systemu SCADA – Supervisory Control and Data Acquisition, a także analogicznych dużych przemysłowych systemów klasy DCS – distributed control system. Warto zwrócić uwagę że system SCADA, podobnie do innych klasycznych przemysłowych systemów kontrolno-pomiarowych jest słabo odporny, jeśli w ogóle, na cyberataki. Tradycyjny system SCADA, oparty na mikrokontrolerach i akwizycji danych DAQ, obejmuje zdalne monitorowanie procesów przemysłowych, sterowanie nadzorcze, raportowanie, oraz alarmy i ostrzeżenia. Urządzenia przemysłowe, poprzez programowalne sterowniki logiczne PLC lub zdalne jednostki końcowe RTU były połączone z systemem komputerowym fabryki. Połączenia stosowane były kablowe wykorzystując popularne magistrale Modbus, Profibus, RP-570, Conitel, protokoły PCN, TCP, systemy Sonet/SDH, a także bezprzewodowe sieci informatyczne OPC – OLE for Process Control. Taka architektura i zestaw jej funkcji zwiększał autonomię systemów przemysłowych oraz obniżał ich koszty utrzymania i operacyjne. IoT rozszerza znacznie te funkcje na inteligentne połączenia, agregację, transformację i przetwarzanie danych, analitykę predykcyjną, analitykę doradczą, tworzenie nowych wartości z danych, oraz budowanie nowych modeli biznesowych.

Podobna sytuacja, jak przedstawiono dla SCADA, czyli ewolucyjnej transformacji do IoT, dotyczy także innych najbardziej popularnych protokołów komunikacyjnych sieci przemysłowych, takich jak HART, HARQ, Modbus, itp. HART – highway addressable remote transducer jest cyfrowym protokołem dwukierunkowym przeznaczonym do kablowych połączeń pomiędzy urządzeniami inteligentnymi, korzystającym z zastanych kabli analogowych i obsługuje obecnie prawdopodobnie większość urządzeń przemysłowych pracujących w zastanym standardzie sygnałowo prądowym 4 – 20 mA. Można wręcz powiedzieć, że bez HART i jego wersji HART-IP, oraz WirelessHART, nie byłoby obecnie cyfrowej komunikacji w dużych obszarach przemysłu. A cyfra i inteligencja są wymaganym i podatnym podłożem na dalszą sprawną transformację IoT. Tam w przemyśle gdzie jest tylko cyfra i standardowa wolna i prosta komunikacja M2M stosuje się prosty protokół MQTT. Tam gdzie panują zastane starsze standardy przemysłowe nie jest to bezpośrednio możliwe. W nauce do budowy eksperymentów stosowano systemy klasy DCS np. EPICS, DOOCS i inne. One także podlegają transformacji do IoT. Zakładając tylko 1% wzrost efektywności przemysłu po transformacji do IIoT, analiza firmy GE lidera przemysłowej transformacji IoT dotycząca sektorów ropa i gaz, energia, ochrona zdrowia, lotnictwo i kolej, ocenia oszczędności rzędu kilkuset miliardów dolarów w skali globalnej do roku 2030. Co obecnie stanowi najpoważniejsze przeszkody transformacyjne przemysłu? Fragmentacja rynku i technologii wyraża się znaczną różnorodnością, niezależnością i niekompatybilnością sprzętu, oprogramowania, protokołów logistycznych. Rozwój technologii M2M/IoT jest jednak dość złożony, wymaga opanowania przez przemysł nowych umiejętności w sensie wykorzystania innego sprzętu, oprogramowania, systemów wbudowanych, technik komputerowych i telekomunikacyjnych. Obecnie zaledwie kilkanaście procent systemów przemysłowych podlega lub zostało ostatnio transformowanych, pozostałe to systemy poprzednich generacji. Wiele z nich czeka na transformację.

Dalsze przykłady ewolucyjnej transformacji IoT i IIoT są związane z wykorzystaniem innych zastanych, popularnych, sprawdzonych i dobrze działających systemów przemysłowych własnościowych i powszechnych, np. GIS – geograficzne systemy informacyjne, i wielu innych. W praktyce możliwe są także znacznie bardziej skomplikowane ścieżki i scenariusze transformacji przemysłowej IoT. Zawsze jednak w metodzie ewolucyjnej dodaje się nowe czujniki do istniejących sieci sterowania. Buduje się systemy bezprzewodowe czujników rozszerzające obszar obserwowany przez operatora oraz zwiększający możliwości monitorowania pracy maszyn i urządzeń, wzbogacający scentralizowany ośrodek monitoringu. Dodaje się uzupełniające podłączenia odległych infrastruktur jak zbiorniki, magazyny, stacje pomp i pojazdów. Taki proces konwersji i aktywacji rzeczy nazywamy także „serwicyzacją”, czyli w najprostszym przypadku dodaniem do urządzenia możliwości jego zdalnego monitoringu i serwisowania. Nie tylko aktywujemy rzecz ale umożliwiamy jej monitoring, nawet wielu stanów, oraz zdalne serwisowanie. Dostawcy urządzeń przemysłowych IoT oferują serwicyzację prowadzoną przez siebie ale na terenie i w obiekcie klienta jako usługę utrzymania urządzania w ruchu i monitoringu prewencyjnego, zapobiegawczego. Kiedyś koszty dodatkowego, rozproszonego oczujnikowania były duże. Koszty wdrożenia i wykorzystywania czujników gwałtownie spadają, nadarza się więc okazja do zbierania coraz większej ilości danych. Dawniej personel fabryk przy podłączaniu czujników do systemów sterowania i monitorowania oraz oprogramowania analizującego dane mógł wykorzystać tylko standard prądowy 4...20 mA, technologię/protokół HART, lub inne protokoły obiektowej magistrali danych jak fieldbus. Dzisiaj da się zastosować wiele typów i metod połączeń przewodowych oraz bezprzewodowych, często wykorzystując jednocześnie wiele sieci w jednej fabryce.

Bardzo silnym motorem transformacyjnym i aplikacyjnym IoT są platformy internetowe gromadzące i popularyzujące „Przypadki Użycia” aktywacji rzeczy opisane czasami zgodnie ze standardem zunifikowanego języka modelowania UML. Takich platform jest wiele, oficjalnych, konsorcyjnych, społecznościowych, oraz firmowych. Część została wymieniona poprzednio. Można wymienić kilka innych: satori, aylanetworks, libelium, resiot, cumulocity, aries-embedded, panStamp, itp. Warto wymienić hiszpańską platformę thethings.io oferującą gotowe bloki oprogramowania API do łączenia wielu urządzeń IoT oraz związane z nimi przypadki użycia w takich sektorach jak: rolnictwo, przemysł wytwórczy, sektor innowacji i prototypowania, logistyka, oraz inteligentne miasta i budynki. IoT APIs nazywane są managerami lub aktywatorami rzeczy. API planuje funkcje, ‘ożywia’

rzecz, łączy ją z siecią, odczytuje i zapisuje dane, zmienia stan rzeczy, pozwala na subskrypcję kanału rzeczy, oraz co najważniejsze umożliwia, jeśli to jest potrzebne, wizualizację lub analizę danych dostarczanych przez rzecz. Oprogramowanie jest kompatybilne z wieloma głównymi platformami sprzętowymi i programistycznymi jak Arduino, Raspberry Pi, Atmel, ESP8266, Econais, Electric Imp, Intel Edison, Sigfox, itp. Specjalną wersją Arduino, przygotowaną do zastosowań w warunkach przemysłowych IoT jest Industruino posiadające funkcjonalności PLC, i dostępne komercyjnie w kilku wersjach, np. z łączem Ethernet, USB, czy otwarty do prototypowania. Jest to kompaktowy układ programowalny bezpośrednio przez USB bez potrzeby stosowania programatora. Warto zwrócić uwagę na proporcje cen urządzeń laboratoryjnych i przemysłowych. Cena mikro-płyty funkcjonalnej uprzemysłowionej spełniającej odpowiednie standardy może kosztować kilkadziesiąt razy więcej niż płyty laboratoryjnej. Tego typu kompaktowe układy wdrożeniowe IoT o zaawansowanych funkcjonalnościach posiadają podobne charakterystyki więc warto podać je jako dobry przykład. Układ Industruino znakomicie nadający się do IoT-yzacji urządzeń laboratoryjnych i przemysłowych jest wyposażony w osiem uniwersalnych wejść/wyjść cyfrowych I/O 18 i 12 bitowych, cztery wejścia analogowe i dwa wyjścia analogowe oraz izolowany port szeregowy RS485 half-duplex. Porty I/O są, zgodnie ze standardami przemysłowymi, zabezpieczone prądowo, napięciowo, zwarciowo i termicznie. Odrębne trzy strefy funkcjonalne urządzenia, analogowa, cyfrowa i mikrokontrolera Atmega, są odseparowane galwanicznie. Wielką zaletą Arduino/Industruino jest jego znaczna popularność w przemyśle i laboratoriach prototypujących i stąd bierze się dostępność dużych zbiorów bibliotecznych gotowego oprogramowania otwartego. Industruino jest całkowicie kompatybilny z systemami przemysłowymi poprzedniej generacji. W wielu przypadkach można go po prostu włączyć w to samo miejsce gdzie rezydował poprzednio stary sterownik. Obsługuje przemysłowe standardy montażu, poziomy sygnałów logicznych i zasilania jak: montaż DIN, przyciski membranowe, lokalny wyświetlacz stanu, poziomy sygnałowe 0-10 V/4-20 mA, izolacyjność >1 kV, zasilanie 6,5-30 V, wyjściowy zakres napięciowy 3,3-32 V, prąd wyjściowy w indywidualnym wyjściu 2,3 A, całkowity prąd wyjściowy 6 A.

Jak napisać interfejs aplikacyjny API dla swojego własnego przypadku aplikacji IoT, testowej lub rzeczywistej, sprawdzonej, niezawodnej, przemysłowej? Jak potem sprawdzić poprawność tego API? Po pierwsze, zamiast pisać można skorzystać z tysięcy gotowców opublikowanych w otwartych bibliotekach IoT API. Z terminem API związany jest termin SDK software development kit. Część z bibliotek wymieniono poprzednio, ale jest ich znacznie, znacznie więcej, dobrze uporządkowanych tematycznie. Przykładowe, bogate biblioteki IoT API, z szerokimi instrukcjami i wyjaśnieniami znajdują się np. na portalach: zettajs.org, programmableweb.com, iot-ticket.com, hackster.io, vrest.io, developers.nest.com, iotone.com, i wielu innych. Niektóre z portali są hubami API, gdzie swoje urządzenie można podłączyć do zdalnego API IoT rezydującego w chmurze. API pisane w architekturze REST – representational state transfer, określane jako RESTful APIs, są łatwe do formalnego, automatycznego sprawdzania poprawności. Większość najprostszych API traktuje rzecz jako źródło danych. Po drugie, można przeczytać jedną z licznych książek dotyczących podłączania rzeczy do IoT, a w tym pisania API, korzystania z przyjaznego dla użytkownika SDK i po prostu napisać. Po trzecie kupić jakiś przyjazny oprogramowany interfejs sprzętowy z załączoną kolekcją typowych API. Wręcz uroczym i przyjaźnie edukacyjnym przykładem w tym względzie jest zestaw Raspberry Pi. Nawiązuje on do technik redaktora Adama Słodowego prezentowanych dawno temu w telerankowym programie TV „Zrób to sam”, i być może pamiętanych przez starszych czytelników, wielbicieli majsterkowania. Tak, nie ma w tym pomyłki, znaczne obszary IoT są dzisiaj, dzięki dostępności cegiełek składowych, domeną domowego, i to relatywnie prostego majsterkowania. Radość z samodzielnego dodawania nowych funkcjonalności starym przedmiotom jest przeogromna. A duma z zamiany starego monitora komputerowego w smart IoT TV może być jeszcze większa. Mało tego, całkiem nowy telewizor, ale jednak kilkuletni może dostać nowe funkcje wprowadzone ostatnio, a niedostępne w tym modelu. Parafrazując Cosi fan tutte, można powiedzieć, może jeszcze nie wszyscy, ale wielu to robi, i jest to jeden z potężnych oddolnych mechanizmów transformacji naszego pasywnego otoczenia rzeczy w kierunku aktywnego IoT. Tak się dzieje w naszych domach, gdzie zadanie wykonuje z ciekawości pokolenie cyfrowe. Tak też dzieje się w przemyśle wytwórczym. Własnymi siłami można dokonywać obecnie całkiem poważnych transformacji przemysłowych systemów kontrolno-pomiarowych, właśnie ze względu na powszechną dostępność pełnych zestawów API. Tak się dzieje w biznesie informatycznym, w mniejszych firmach wytwórczych. W większym przemyśle wytwórczym możliwy jest outsourcing lub subskrypcja gotowych rozwiązań oferowanych przez dużych dostawców rozwiązań IoT pod klucz. Dobrym przykładem niedawnej transformacji z sukcesem do poziomu IoT dużego sektora przemysłu jest energetyka wiatrowa w USA, przekraczająca obecnie 80 GW i rozwijana od ponad 30 lat. Dostarcza ona ok. 230TWh, co stanowi ok. 6% rynku. Wszystkie starsze farmy wiatrowe były zarządzane do niedawna „ręcznie”, co czyniło system mało elastycznym, z dzisiejszego punktu widzenia powiedzielibyśmy że archaicznym. Włączenie lub wyłączanie odległego o wiele kilometrów generatora wymagało wizyty technika in situ. Tysiące starszych generatorów zostało ostatnio podłączonych do sieciowego energetycznego systemu IoT. To co zostało zrobione w powyższym przypadku jest najprostszą formą transformacji IoT i jest nazywane aktywacją, ożywieniem, funkcjonalizacją, multi-funkcjonalizacją, re-funkcjonalizacją, lub, jak już wspomniano, serwicyzacją rzeczy. Te terminy związane z IoT nie są identyczne, nie oznaczają tego samego, gdyby trzeba i można byłoby rozważać je głębiej i w detalach. One wyznaczają różne ścieżki IoT-yzacji przemysłu.

IoT posiada poważny potencjał transformacyjny modeli biznesowych (Kranz 2016). Kluczem są wysokiej jakości dane. Dzięki zastosowaniu takich technik bazujących na danych jak adaptacyjnej analityki i utrzymania predykcyjnego rynek będzie systematycznie przesuwany od sprzedaży aktywów do sprzedaży usług. Dzisiaj przeszkodą szybkiej transformacji, jak już wspominano, jest wiek zastanego przemysłu i często znaczna inercja skomplikowanych i kosztownych procesów konwersji infrastruktury sprzętowej i programistycznej. Także czasami inercja kadry. Szczególnie dotyczy to dużych, mało ruchliwych sektorów przemysłu wytwórczego jak generacja energii, pozyskiwanie surowców, wielkoskalowej automatyki przemysłowej itp. Mówimy wówczas także o bardziej lub mniej standaryzowanych kolorowych procesach transformacji przemysłowej – brązowych i zielonych. Niby to jest cały czas to samo, o czym pisano powyżej w odniesieniu do aktywacji rzeczy, ale zastosowanie rynkowo zorientowanej terminologii kolorowej rzuca na procesy transformacji IoT być może nieco inne światło. W takich procesach transformacji liczy się nie tylko ich treść, ścieżka i technologia, ale i kontekst, oraz psychologia, i techniki rynkowe. Transformację IoT/IIoT pod klucz ‘brown to green’ oferuje wiele firm komercyjnych, jak np. Intel Wind River, Trace Software, i inne. Obszarem brązowym nazywa się przemysł klasyczny z miliardami dyskretnych urządzeń i aplikacji programistycznych pracujących w izolacji, indywidualnie, autonomicznie. Wiele z tych elementów będzie wymagać migracji pozwalających na skorzystanie z zalet IoT. Obszar brązowy jest określony historycznie. Obszarem zielonym nazywa się urządzenia przemysłowe budowane od podstaw w postaci kompatybilnej ze standardami IoT. Są to urządzenia podłączone do sieci, które powinny być bezpieczne, oraz zarządzane zdalnie. Obszar zielony jest całkowicie oddzielony od poprzednich rozwiązań. Transformacja obszarów brązowego do zielonego może przebiegać kilkoma drogami, w pewnym sensie pojedynczo, indywidualnie, skromniej, prościej i taniej lub całościowo, holistycznie, z perspektywą przyszłościową. Najprostszym i najszybszym rozwiązaniem jest dodanie bramki sieciowej przesyłającej odczyty urządzeń do chmury, gdzie wykonywana jest inteligentna analityka. Jest to podejście izolujące kolory brązowy od zielonego. Obszar graniczny jest wyznaczany przez bramki sieciowe. Obszar brązowy zachowuje granice i poprzednie technologie ale jest unowocześniony i aktywowany. Warunkiem sukcesu takiego rozwiązania jest cały czas tkwiący potencjał funkcjonalny, produkcyjny i inny w obszarze brązowym, i w związku z tym opłacalność takiej transformacji brązowej. Brązowa transformacja holistyczna wymaga zastosowania platformy lub ekosystemu IoT. Platforma jest elastycznym środowiskiem wykonawczym aplikacji, różnych urządzeń, elementów funkcjonalnych systemu przemysłowego i warstw sieci operacyjnej. Elastyczność platformy jest określona poprzez modularną konstrukcję i uniezależnienie rozwoju aplikacji od rdzeniowego API systemu operacyjnego. Platforma, bazująca na systemie operacyjnym czasu rzeczywistego może znajdować się w chmurze, w routerze lub bramce sieciowej, a także na poziomie samego urządzenia. Platforma może być zlokalizowana wewnątrz firmy, jak jest często w przypadku dużych przedsiębiorstw, lub być otwarta na zasadzie usług zewnętrznych zapewnianych przez dostawcę sieciowego IoT. Działanie na elastycznej platformie IoT posiada wiele zalet dla obszaru brązowego. Umożliwia firmom samodzielne pisanie aplikacji, przesuwanie ich pomiędzy różnymi warstwami funkcjonal-

nymi, pozwala redukować koszty transformacji i jej skalowania, oraz dodawać nowe rozwojowe funkcjonalności rozszerzające platformę. Uniwersalność i standaryzacja platformy IoT umożliwia dzielenie aplikacji z innymi. Następnym etapem transformacji holistycznej jest wirtualizacja umożliwiająca całkowitą separację oprogramowania od sprzętu platformy i systemu operacyjnego. Wirtualizacja przełamuje paradygmat urządzeń obsługujących jedną funkcję, zamieniając je w systemy wielofunkcyjne, a przez to umożliwiając konsolidacje wielu aplikacji i wielu systemów operacyjnych na jednej platformie. Wirtualizacja, przez 'intelektualizację' funkcjonalności, skokowo o rzędy wielkości zmniejsza zapotrzebowanie systemów na przestrzeń, czas, ilość zaangażowanej materii i zużycie energii. Wirtualizacja to także umieszczenie pracochłonnych, masowych, szybkich standardowych funkcji w sprzęcie a rozmaitości i wirtuozerii intelektualnej w oprogramowaniu. Wirtualizacja to głęboko optymalizowane współ-projektowanie sprzętowo- programistyczne systemów funkcjonalnych. Wirtualizacja, ściśle związana z transformacją obszarów brązowych IoT w zielone, umożliwia ruchomość funkcjonalności w sieci, nie tylko elementarne przesunięcie funkcji z urządzenia do sieci, ale optymalne umiejscowienie funkcji w odpowiedniej lokalizacji sieci. O sieci takiej, wyposażonej także w warstwę zarządzania urządzeniami, funkcjami operacyjnymi i atrybutami procesów, mówimy że posiada architekturę zorientowaną usługowo. Procesy transformacji kolorowej brązowo-zielonej IoT są dokładnie analizowane przez rynki gospodarcze, finansowe i biznesowe gdyż globalna wartość tych przemian jest gigantyczna, i powinny one dokonać się w sposób najbardziej intensywny najbliższym dziesięcioleciu.

W transformacji IoT, CIoT i IIoT wiodącą rolę odgrywają tzw. obszary IoT intensywne. Wyżej wymieniono nasze miejsce zamieszkania jako obszar IoT intensywny. Wśród takich obszarów jednym z najszybciej podlegających transformacji jest sport. Internetyzowane jest ciało sportowca i ubranie, a w tym koszulki, spodenki, kostiumy pływackie i kąpielowe, obuwie, wkładki do obuwia, poprzednio wymienione zegarki, bransoletki i opaski, inne części ubrania. Internetyzowany jest sprzęt sportowy. Czujniki, podłączenie do sieci, zbieranie danych, analityka w warstwie wyższej jest dostępne w takich urządzeniach jak: sprzęt siłowy, hantle, sztangielki, ciężarki sportowe, sprzęt na siłownię, gryfy, wędki sportowe, bramki do gier zespołowych, tablice i kosze do koszykówki, piłki, rowery i rowery stacjonarne, rowerowe zamki bezpieczeństwa, siodełka rowerowe, amortyzatory rowerowe, kaski rowerowe, urządzenia do nurkowania, akwalungi, różnego rodzaju rękawice sportowe – rowerowe, ciężarowe, bokserskie, narciarskie, worki bokserskie, oprzyrządowanie sportów walki, hełmy sportowe, kajaki, łyżworolki i deskorolki, narty i deski narciarskie, deski surfingowe i narty wodne, buty do biegania, skakanki sportowe, bieżnie stacjonarne i dynamiczne, maty sportowe, oraz sprzęt sportowy zaprojektowany przez klientów do negocjacji. To nie są żarty, to jest sprzęt sportowy który można dzisiaj kupić w kilku firmach, np. seebo, fitbit, kaa, AMPT – advanced mp technology, i inne. IoT po prostu naprawdę rewolucjonizuje sport. Mówiąc żartobliwie doping sportowy się także IoT-yzuje. Aktywatory dodają początkowo podstawowe funkcjonalności wymienionym przedmiotom stosowanym w sporcie, ale następnie znacznie bardziej zaawansowane. Czujniki w nartach mierzą spektrum drgań narty, obliczają transformatę Fouriera tego spektrum określając rezonanse i główne składniki widma, mierzą energię drgań w poszczególnych częściach widma, wysiłek narciarza, pokonane przewyższenie, nachylenie i ukształtowanie stoku, rozkład przyspieszeń w przestrzeni i czasie, sylwetkę narciarza, jakość śniegu, i wiele innych. Pozwalają na optymalizację jazdy. Bokserski worek treningowy czy mata do sportów walki określają dość dokładnie profil fizyczny zawodnika. Mierzą rozkład czasu, kierunków, siłę i częstotliwość uderzeń zawodnika, określają taktykę działania sportowca. Wkładki do obuwia mierzą wiele parametrów mechanicznych w tym rozkład siły przy różnych rodzajach biegu. Sztangielki mierzą siłę uścisku ręki, przyspieszenie, liczą ruchy, sumują wysiłek i podniesiony ciężar. W czujniki wyposażana jest cala infrastruktura sportowa, stadiony, bieżnie, baseny, boiska, ringi zapaśnicze, rzutnie, itp. Dane zbierane ze sprzętu sportowego i infrastruktury podlegają akwizycji, fuzji i integracji z różnych źródeł, oraz analityce w trybie czasu rzeczywistego. Trwa dyskusja jak sędziować np. mecze piłkarskie. Jak wspomagać sędziego przy pomocy środków IoT czasu rzeczywistego. Ile tam powinno być człowieka a ile IoT. Ta dyskusja będzie trwała jakiś czas i jest wyraźnym znakiem okresu przemiany. Poważnym pytaniem na dzisiaj jest kiedy człowiek w tych decyzjach w sporcie, ruchu drogowym, a później szerzej np. w medycynie, zostanie zmarginalizowany. Inne obszary szybko transformowane to właśnie medycyna, teren szpitala, laboratoria, sale operacyjne, a także sale pacjentów, intensywna terapia medyczna, wyposażenie szpitalne, łóżka specjalizowane, monitorowanie specjalistyczne obszarów przebywania pacjentów. Kolejne obszary to gęsta i tzw. intensywna przestrzeń miejska, w tym centra i galerie handlowe, oraz supermarkety, lotniska, stacje metra, masowe obiekty kultury. Tam nasycenie IoT będzie wrastało przez najbliższy czas najbardziej i pod względem wyposażenia w struktury inteligentne będzie wyprzedzać znacznie inne obszary. Niektóre firmy IoT działające w wymienionych tutaj intensywnych obszarach implementacji IoT wyprzedzająco uczą rynek, zakładając 'Akademie IoT' gdzie klient ma dostępne tutoriale na temat przypadków użycia urządzeń IoT, tutoriale projektowania urządzeń, pisania własnych aplikacji, rozwoju systemów wbudowanych, szybkiego prototypowania, wydobywania informacji z danych i wykorzystanie ich do analityki czasu rzeczywistego, czyli w skrócie aktywacji przedmiotów i dodawania im nowych funkcjonalności lokalnych i przydatnych hierarchicznie wyżej do analiz agregacyjnych. Dostępne są także komercyjnie rozszerzone analizy wybranych przypadków zastosowania IoT zakończone sukcesem, ale też niepowodzeniem.

Amazon jest obecnie największym sprzedawcą internetowym na świecie. Obsługując kilkaset milionów ludzi wyznacza także kierunki rozwoju usług IoT/CIoT prowadząc własne zaawansowane badania nad behawiorystyką różnych grup klientów, oraz systemami sprzętowymi i programistycznymi logistyki. Działa poprzez dostępny dla klientów i operatorów system usług sieciowych AWS – Amazon Web Services. AWS IoT posiada wiele funkcjonalności zgrupowanych w trzy płaszczyzny: Greengrass, IoT Platform i IoT Button. Funkcjonalność zielona jest oprogramowaniem rozszerzającym AWS na odwiedzaną przez klienta platformę WWW, oraz podłączone urządzenia i sprzęt. Odwiedziny portalu i zainteresowanie produktem mogą uaktywniać aktywność typu inteligentne oddzwanianie. Platforma IoT udostępnia klientom funkcjonalność zaawansowanej chmury. IoT Button jest oprogramowaniem działającym na sprzęcie Wi-Fi Dash Button i umożliwiającym proste korzystania z sieciowych usług firmy. W nieco inny sposób, ale także w obszarze IoT działają także wielkie sieci handlowe jak Walmart, Auchan, Carrefour, Tesco, i inne. Walmart prowadził robotyczne, samojezdne inteligentne wózki sklepowe podążające za kupującym, pokazujące sumowaną kwotę zakupów, i zapamiętujące w systemie zwyczaje klienta. Potencjał takich wózków jest znaczny i obejmuje: zastępowanie pracy wielu osób obsługujących supermarket, w tym przenoszenie towarów, porządkowanie półek, dostarczanie na żądanie, monitorowanie zapasów, itp. Auchan wprowadza eksperymentalnie system e-marketingu Proximity Shopping. Współpracuje z Orange Business Services w masowym wprowadzeniu technik RFID do optymalizacji logistyki. Carrefour wdraża plan cyfrowego marketingu polegający na zmianie sklepów w inteligentne magazyny zarządzane IoT. Tesco analizuje zmiany przyzwyczajeń zakupowych klientów, zwracając jednak uwagę na ciągłą przewagę wizyty klienta w supermarkecie. Jednak oczekiwania klienta odnośnie takiej wizyty znacznie się zmieniają. Dla klienta Tesco prowadzi interakcyjny serwis IoT IFTTT.com – If This Then That. Wszystkie wymienione systemy bazują na zbieraniu znacznych ilości danych. Ruchy i zachowania klienta, obsługi, towarów są śledzone radiowo, dokumentowane w bazie danych i analizowane wielopłaszczyznowo. Analizy dotyczą na przykład zagadnienia rekomendacji podczas zakupów, co jest obecnie typowym jednak bardzo skomplikowanym problemem IoT. Skomplikowanym, ponieważ dotyczy oddzielenia przypadkowości od zachowań systematycznych i prób modelowania zachowań przypadkowych. IoT tworzy nowe wartości w handlu detalicznym, np. takie jak: predykcyjne utrzymanie wysokiej jakości towarów, monitoring zapasów towarowych, optymalizacja czasu pracy personelu, osobiste doradztwo klientowi, nigdy więcej czekania w kolejce, transformacja modeli biznesowych, itp. Klient w swoim portfolio zakupowym może wydawać bardzo złożone żądania warunkowe lub sprzężone, np. włóż do koszyka wybraną paczkę łososia wędzonego we wtorek jeśli będzie promocja lub cena spadnie o 10%, ale tylko wtedy jeśli jednocześnie zakupię sos tatarski, i jeszcze mam w lodówce szpinak!

Wśród kilku możliwych scenariuszy rozwojowych IoT/IIoT w relatywnie bliskiej skali czsowej rozważana jest, jako dość prawdopodobna, wersja kognitywna CIoT (Balani 2015). Opracowywane są teoretycznie nowe paradygmaty (Wu 2014), i optymalizowane architektury CIoT (Zhang 2015). Mówi się o perspektywnie dekady, jako horyzoncie znaczej popularyzacji tego rozwiązania, choć wiele indywidualnych rozwiązań o lokalnej skali funkcjonuje już dzisiaj i to całkiem efektywnie. Czasami w odniesieniu do takich systemów, szczególnie w inteligentnym transporcie ITS, używany jest termin i skrót iCPS

(także iPCS, iCPSS, PSS, mobile CPS) – inteligent-cyber-physical-social. Wersję kognitywną IoT obarcza się zadaniem dokonania praktycznej konwergencji technologicznej i funkcjonalnej wielu różnych technologii, oraz wykorzystania istniejących bądź rozwijanych platform posiadających atrybut kognitywności do swojego rozwoju. Wśród tych składowych mających złożyć się na kognitywność IoT wymieniane są: inteligentne czujniki, ale nie aktywowane ale inherentnie technologicznie inteligentne; kognitywne media; sieci świadome na wszystkich poziomach ruchu i dla wszystkich funkcji – proksymalne, dostępowe i transportowe; urządzenia, oprogramowanie, mobilna inteligencja obliczeniowa, itp., konwertowane do usług świadomych; odzyskiwanie, pobieranie i lokalna generacja energii – świadoma gospodarka energią, itp. Przez CIoT rozumiemy IoT o mniej więcej następujących atrybutach: dynamicznie konfigurowany, świadomy świadczonych usług, optymalizujący użycie posiadanych zasobów, odkrywający zasoby i funkcjonalności w swoim otoczeniu, zmieniający swoje wewnętrzne i zewnętrzne parametry operacyjne i funkcjonalne do potrzeb, wykorzystujący dane generowane z obszarów brzegowych do zmian decyzji i funkcji w czasie rzeczywistym, reagujący na zapotrzebowanie funkcjonalne w sposób 'inteligentny', zdolny bo bezpośredniej i aktywnej interakcji z człowiekiem na wielu poziomach informacyjnych; uczący się nowych sytuacji, funkcji, reakcji, szybko relokujący zasoby w razie potrzeb, itp. Na poziomie interakcji z człowiekiem CIoT ciągle nadąża za nim uruchamiając standardowe funkcjonalności w biegu, przewidując i ewentualnie uruchamiając funkcjonalności sytuacyjne, oczekując i wykazując gotowość na działania dynamiczne w czasie rzeczywistym. Na poziomie infrastrukturalnym, biznesowym i przemysłowym CIoT wspomaga, przewiduje, uprzedza, wyprzedza, rozróżnia i rozpoznaje sytuacje, zapobiega, dostarcza przetworzone dane, optymalizuje działania gospodarcze, analizuje dane i sytuacje, wykorzystuje analitykę do wspomagania podejmowania decyzji, proponuje rozwiązania, ostrzega, zapobiega sytuacjom krytycznym, itp. Konsumpcyjne rozwiązania CIoT proponuje już wiele firm dowstawców usług IoT. W masywne wielkoprzemysłowe aplikacje CIoT angażują się równie wielkie firmy ICT. Cisco prowadzi badania o miliardowej skali i podejmuje wysiłki aplikacyjne kognitywnych platform IoT, np. Cisco Jasper, na poziomie wielkiego ruchu transportowego i wielu sektorowych zastosowań przemysłowych (jasper.com). IBM równie masywnie pracuje nad swoim oprogramowaniem np. grupą Watson API (Fisher 2015), a także systemowymi ukierunkowanymi rozwiązaniami CIoT sektorowymi np. dla przemysłów wydobywczych ropy i gazu, chemicznego, farmaceutycznego, a także dla przemysłu samochodowego (Womack 2016). Watson APIs potrafią komunikować się z człowiekiem zaawansowanym językiem naturalnym, rozumieją obrazy, rozpoznają sceny, uczą się z masywnych danych czujnikowych, znajdują sensowne wzory danych, tworzą informacje z danych, korelują dane z zewnętrznymi źródłami danych, komunikują się z mediami społecznościowymi, jak Twitter, FaceBook, korzystają z prognoz pogody, itp. Zwykły IoT w tych sektorach już dzisiaj nie wystarcza, musi być kognitywny! Ewolucyjna ścieżka transformacji przebiega od pasywnych, ale już jakiś czas temu usieciowionych systemów pomiarowych, do systemów wypasażanych w coraz bogatsze, aktywne warstwy kognitywne bazujące na uczeniu maszynowym i wielkich zbiorach strukturyzowanych i niestrukturyzowannych danych, które rozumieją powód swojego działania i wspierają podstawowe funkcjonalności całego systemu coraz lepiej szybkimi i skutecznymi działaniami prewencyjnymi, oraz wypracowanymi rekomendacjami. Dzisiejsze rekomendacje, warte czasami w dużym przemyśle miliony, zamienią się prędzej czy później w aktywne autonomiczne działanie. Wymienione opracowania sektorowe z żadnym przypadku nie mają charakteru futurystycznych szacowań rynków. Podawane są dokładne opisy implementacji prototypowych, precyzyjne dane dotyczące parametrów, zatrudnienia i ekonomicznych transformacji IoT[C] dla niektórych sektorów przemysłu, np. takie jak ekwiwalenty zatrudnieniowe, zwrot na inwestycji ROI, itp.

Combat cloud jest jednym z potencjalnie najpotężniejszych frontów obronnych militarnych zastosowań IoT. W wojsku wszystko staje się w przyszłości IoT. Czy można wypuścić na morze korwetę wartą wiele miliardów Euro bez zdalnego zabezpieczenia o charakterze lokalnym i szerszym? Mówiąc nieco w przenośni, nadziała by się na dobrze zrobioną minę plastikową lub dostała by taką rakietką za parę tysięcy euro. Chodzi o stosunek kosztów i życie ludzkie. Ten wygrywa kto pokona przeciwnika wirtualnym wzrokiem, słuchem i innymi zmysłami, także czasem, szybkością reakcji, koncentracją i relokacją siły, kto ma znacznie lepszy stosunek kosztów. To wszysko są atrybuty IoT. Korweta musi być dobrze otoczona dronami powodnymi i zabezpieczona w wodzie i z powietrza na różnych horyzontach odległościowych. Musi być wokół zamknięty w pełni funkcjonalny, szybko reagujący system IoT. Jak zabezpieczyć wyborowego snajpera na wysuniętym stanowisku? Nie ma on oczu na plecach i po bokach. Nie ma uszu za sąsiednim drzewen. Musi być wspierany IoT. Musi być otoczony rozsiewaną osobistą siecią obronną, w tym dynamicznie podnoszonymi w razie potrzeby nanodronami, ewentualnie zdolnymi do ograniczonego zaatakowania i obezwładnienia pojedynczych żołnierzy wroga. Czasami ten jeden jedyny strzał snajpera musi być aż tak znacznie wspierany logistycznie. Jak zaostrzyć swój daleki wzrok jeśli nie korzystając z technologii multi i hiperspektralnych wspomaganych masywnymi obliczeniami wspomagającymi w czasie rzeczywistym w mgle i chmurze? W tych obliczeniach musimy uwzględnić korekcję atmosferyczną, lokalizację geograficzną, porę roku, klimat, pogodę, porę dnia, wilgotność, chmury, słońce, kierunek oświetlenia, roślinność w otoczeniu akwizycji danych, odległość obserwacji, i parę innych rzeczy. IoT obronny jest jednym z najpotężniejszych mechanizmów i frontów rozwojowych obecnych technologii IoT.

Eppur si muove IoT

Zapewne nie wszyscy czytelnicy zgodzą się z tezą, że być może jesteśmy świadkami początkowej fazy rodzaju przewrotu kopernikańskiego, gdzie w jakiejś przyszłości, uwzględniając jednak skalę aby nie popaść w śmieszność, IoT jak Sol omnia regit. Sceptycy powiedzą stanowczo, że to duża przesada. Nie wiemy jak daleko wybiegamy w przyszłość? Wszystko zależy od człowieka. Możemy wstrzymać postęp lub zasadniczo zmienić jego kierunek. Zdefiniujmy jednak IoT znacznie szerzej niż to obserwujemy i rozwijamy dzisiaj. IoT nazwiemy wkrótce inaczej i stanie się on, jeśli do tego dopuścimy, inteligentnym środowiskiem życia człowieka. Człowiek może dążyć do tego aby to środowisko było co najmniej tak inteligentne jak on, aby móc nawiązać z nim kontakt intelektualny, dyskusję. Przypomnijmy zatem dla takiego upodmiotowionego środowiska kilka fundamentalnych argumentów i zadajmy kilka pytań, oczywiście nie odpowiadając na nie. Co może powstrzymać rozwój sztucznej inteligencji i środowiska? Pierwsza poważna katastrofa w tym obszarze? Jak poważna musi to być katastrofa? Może wystarczy nam dokładne zdanie sobie sprawy ze skali zagrożenia, i proporcji pomiędzy potencjalnymi korzyściami a niebezpieczeństwem? A może wcale nie ma żadnego zagrożenia? Co się stanie jeśli zaczniemy masowo drukować zaawansowaną sub-inteligentną elektronikę bardzo tanio i wyposażać w nią środowisko? Co się stanie jeśli plan Elona Muska umieszczenia na orbicie wielu tysięcy szerokopasmowych satelitów zostanie zrealizowany i po pewnym czasie w ogóle i na zawsze zapomnimy co to jest ograniczenie pasma transmisyjnego? Czy inteligencja i jej emocjonalny obszar jest wyłącznym atrybutem Homo sapiens sapiens? Kto dzisiaj odważy się dać odciąć sobie głowę za obronę tej tezy? Kto odważy się torturować apologetów tezy przeciwnej? Jaki system prawny musimy wprowadzić i jak go uzasadnić aby wstrzymać rozwój inteligentnego środowiska? Czy kiedykolwiek ktoś postawi przed sądem i za co pierwszą samoświadomą, autonomiczną sztuczną inteligencję? Kto pierwszy zauważy, jeśli kiedykolwiek do tego dojdzie, wyraźne zagrożenie ze strony inteligentnego środowiska? W jaki sposób dzisiaj egzekwować fundamentalne „Reguły Sztucznej Integencji z Asilomar"?

Ku pamięci, zamiast zakończenia po całym przedstawionym tutaj nieuporządkowanym wywodzie warto może powtórzyć i spróbować zapamiętać dzisiejsze, na razie relatywnie proste, i wyłaniające się już jutro główne zastosowania IoT, o których poprzednio pisaliśmy z konieczności pobieżnie.

– Zastosowania w logistyce związane z lokalizacją i śledzeniem ruchu obiektów, telemetria flot samochodów osobowych, autobusów i ciężarówek, śledzenie ruchu kontenerów, paczek pocztowych;

– Produkcja i zastosowania przemysłowe, sterowanie i działania operacyjne urządzeń przemysłowych, zarządzanie inteligentnymi liniami produkcyjnymi, robotyka przemysłowa;

– Zarządzanie aktywami i inteligentne magazynowanie, dostawa automatyczna z magazynu do miejsc sprzedaży;

– Automatyka budynkowa, inteligentne budynki, systemy monitoringu i kontroli zastosowane do wszystkich urządzań wewnątrz budynku, proaktywne zarządzanie, optymalizacja działania systemów;

– Inteligentne systemy transportu, zarządzanie transportem morskim, drogowym i kolejowym;

– Połączone pojazdy, system informacyjny dla kierowcy, status drogi, czarne skrzynki bezpieczeństwa pojazdu;

– Inteligentne miasta, monitoring i sterowanie w zautomatyzowanych systemach municypalnych służą zwiększeniu sprawności działania i poprawie jakości obsługi mieszkańców;

– Inteligentna sieć energetyczna na wszystkich poziomach, optymalizacja zużycia energii, zarządzanie czasowymi i odnawialnymi źródłami energii;

– Aplikacje konsumenckie, związane ze smartfonami, osobistymi urządzaniami noszonymi, np. portfelem i ubraniem;

– Zastosowania medyczne, zdalny monitoring i terapia pacjentów, wspomaganie osób niepełnosprawnych;

– Handel detaliczny i inteligentne zakupy, wykorzystanie informacji o kliencie w celu kierowania osobistej optymalnej oferty;

– Inteligentne mieszkanie, autonomiczne zarządzanie gospodarstwa domowego, kontrola ogrzewania, kontrola działania urządzeń AGD, zamawianie żywności i produktów domowych;

– Kultura, rozrywka, multimedia, konwergencja mediów, środowiska immersyjne i trójwymiarowe;

– Konwergencja IoT z wieloma technologiami ICT jak GIS, cyberbezpieczeństwo, usługi obliczeniowe, wspomaganie podejmowania decyzji, systemy wspomagania działania biznesowego i gospodarczego;

– Monitoring wielkoobszarowy środowiska naturalnego, samokonfigurujące się sieci czujnikowe, czujniki rozsiewane, samo-zasilające się węzły sieci, czujniki gromadzące energię połączone z technologią wirelessHART, gromadzenie energii z różnic temperatury i wilgotności, rolnictwo precyzyjne;

Konieczne jest uzmysłowienie sobie na koniec jaką Wieżę Babel zbudowaliśmy do tej pory z mieszaniny stosowanych, przeszłych, obecnych, rozwijanych i badanych przyszłych technologii i używanych do komunikacji przy budowie tej wieży języków. Z jaką kakofonią technologiczną musi poradzić sobie IoT jeśli ma odnieść sukces jako wielki integrator i budowniczy nowej prawdziwie konwergencyjnej platformy technologicznej cyfrowego i kwantowego świata. Dodatkowym ciekawym czynnikiem socjologicznym budowy tej Wieży jest fakt, że znaczna część użytkowników indywidualnych w ogóle nie zadaje sobie sprawy z roli i konieczności konwergencji i standaryzacji IoT ani nawet z zasad działania wielu prostych aktywowanych urządzeń. Ale czy musi? Mamy więc do czynienia nie na końcu, jak to było w wieży mitycznej, a już na początku z pomieszaniem i niezrozumieniem języków. Kiedyś pomieszanie języków przeszkodziło, a dzisiaj? Podobnie jak w poprzednich częściach pracy wymieniamy ponownie, z konieczności bez szerszego komentarza, niektóre stosowane liczne języki, standardy i technologie, które mogą być objęte parasolem zarówno brzegowego IoT jak i jego głębszych warstw, grupując je arbitralnie w wybrane platformy funkcjonalne jak np.: sieci ultra-niskoenergetyczne, zdalne zarządzanie urządzeniami, integracja protokołów komunikacyjnych, porty I/O, integracja oprogramowania wbudowanego typu software i firmware, integracja usług CSP – communicating sequential processes dla urządzeń, czujniki i przetwarzanie sygnałów, ekosystemy dla inteligentnego miasta, domu, i inne.

– Sieci sygnalizacyjne sekwencyjne CSP: SIP, SS7, SIGTRAN, ISUP, CAMEL;

– API sieci operatorskich: GSMA, One API, OSA/Parlay WS;

– Komunikacja IP: VoIP, IMS, IPTV, VoD, PTT, OTT, Presence, Messaging;

– Systemy operacyjne best effort i czasu rzeczywistego: mbed, Predix, eCos, Linux, Unix, QNX, Android, Apple OS, Windows, RTOS, VxWorks, FreeRTOS, TI-RTOS, LynxOS, Sirius RTOS, RTAI, RTEMS, RTKernel, IRMX, wolfSSL INtime RTOS, itp;

– Łącza szeregowe: UART, PCIe, USB, SPI, I2C, RS-232, RS-485, 1-Wire, CAN, TTCAN, LIN, MOST, RGMII/SGMII;

– Łącza przewodowe i magistrale przemysłowe: PLC, Ethernet, xDSL, FTTx, DOCSIS, PSTN, Profibus, Fieldbus, Modbus, M-BUS, AS-I, RS, CAN, 1-Wire, VXI, PXI, GPIB, HPIB;

– Łącza bezprzewodowe: IEEE 802.xx, BT, RF, DECT ULE, xG, SatCom, GSM, 4G/5G, Sigfox, Wi-Fi, RFID, Z-Wave, ZigBee, SWAP;

– Zdalne zarządzanie sprzętem użytkownika końcowego: CPE, CWMP, TR-069 i pochodne,

– Telemetria nisko-zasobowa: MQTT, REST API MP;

– Multimedialne sieci domowe: UPnP, DLNA, AirPlay, Miracast;

– Sieci domowe: KNX, X10, BACnet, 802.xx, 6LoWPAN, ZigBee, Z-Wave, Wireless M-Bus, ModBus, M-Bus;

– Magazyny danych i narzędzia komunikacji: NAS, SMB, AFP, WebDav, FTP/SFTP, WinSCP, NFS, DropBox, Box, SkyDrive, OneDrive, Google Drive, Amazon S3;

– Standardy sprzętowe: NIM, CAMAC, FASTBUS, EDS, VME, VME64, NV/mixed, VXI, ATCA, MTCA, i inne;

– Protokoły: 6LowPAN, WiFi, DNS, IP/TCP, MQTT, CaAP, AMQP, RPL, JSON-LD i dosłownie setki innych.

Warto także wykonać, choćby w zarysie i w sposób niepełny analizę SWOT dla IoT, a w zasadzie zasygnalizować konieczność jej zrobienia. W wielu obszarach aplikacji rozwiązania IoT będą bardzo proste. Nazwiemy je trywialnym IoT. W innych będą wymagać znacznej inteligencji obliczeniowej. W pewnych obszarach IoT będzie posiadał charakter pasywny, jedynie wspomagający, w innych wręcz przeciwnie bardzo aktywny, o charakterze decydującym. Obszary aplikacji można podzielić na cztery główne dziedziny: popularne i amatorskie, komercyjne dla masowego rynku konsumenta, usługowe, oraz małe i duże przemysłowe np. dla infrastruktury. Zupełnie inne są mocne i słabe strony takich odmiennych rozwiązań IoT. Zupełnie inne są w takich różnych obszarach szanse i zagrożenia. Można mówić w pierwszym przybliżeniu o trzech poziomach poważnego wpływu IoT na: człowieka, infrastrukturę i środowisko, i związanych z nimi różnych korzyściach i zagrożeniach. Wpływ IoT na środowisko będzie potencjalnie bardzo duży. Obecne urządzenia IoT są dalece nieoptymalne. Nawet jeśli pojedyncze urządzenie zużywa małą moc np. poniżej 1 W, sumując wszystkie etapy działania od mechanizmu pomiarowego, akwizycji, przetwarzania i transmisji danych, do ich interpretacji i wykorzystania, to ile zużywają miliony, a co dopiero miliardy. Są to potencjalnie gigawaty i terawaty. Takiej mocy dzisiaj do swobodnej dyspozycji nie mamy. Koszty wielu gigawatów energii są ogromne, a wytworzenie ich w sposób klasyczny prowadzi do katastrofy środowiskowej. Musimy energię dla przyszłej inteligencji infrastrukturalnej wytworzyć zupełnie inaczej. Niezawodność systemu składającego się z miliardów i dalej trylionów elementów jest dzisiaj niemożliwa do oceny. Wymaga nowej nauki. Kompletnie nie wiemy jak zmieni się człowiek otoczony agresywną inteligencją infrastrukturalną. Czy w ogóle to zniesie, czy przeżyje i jaka będzie jakość tego życia? Czy taka inteligencja pozostanie na poziomie biernym, jedynie wspomagającym? I to wymaga zupełnie nowej nauki. Podsumowując, można spróbować wymienić niektóre elementy SWOT dla IoT dzisiaj i w niedalekiej przyszłości:

– mocne strony: niskie koszty jednostkowe prostych rozwiązań, popularność i moda, szybka i prosta ingerencja w najbliższe otoczenie człowieka, wspomaganie człowieka obecnie w prostych czynnościach,

– słabe strony: wielka różnorodność i niepodatność na standaryzację w większej skali, obecnie znaczne zapotrzebowanie na energię, nieoptymalne rozwiązania indywidualne, spontaniczny i zabałaganiony rozwój,

– szanse: rozwój cywilizacji, poprawa warunków i możliwości gospodarowania człowieka, potencjalny znaczny wpływ na rozwój medycyny i poprawy zdrowia człowieka, pokonanie barier technologicznych w obszarze, energii, transportu, zdobywania nowej wiedzy, ułatwienie codziennego życia człowieka, ożywiona reagująca funkcjonalnie infrastruktura wokół człowieka,

– zagrożenia: potencjalnie znaczny i bezpośredni wpływ na człowieka, znaczny wpływ na środowisko naturalne, nieznane i trudno przewidywalne kierunki masowego rozwoju, agresywność niektórych rozwiązań IoT, hiper-masowy Internet satelitarny obsługiwany przez tysiące satelitów zamieni wszystko w dane, potencjalna możliwość utraty kontroli nad danymi, wszechobecny nadzór człowieka przez IoT,

Analiza SWOT jest dzisiaj wiarygodna tylko dla wąskich sektorów IoT. Ogólna ma jedynie charakter informacyjny. Konieczne byłoby znalezienie powiązań pomiędzy poszczególnymi składnikami, nawet wydawałoby się odległymi. W przypadku elektronicznych ubrań, przewidując rozwój tej technologii i jej zastosowań, można oceniać jej wpływ na medycynę, monitoring i wspomaganie pacjentów, zmiany warunków pracy człowieka, zmiany w obszarze BHP, sporcie, zachowaniu i następnie przyzwyczajeniach człowieka, itp. Technologie elektronicznych ubrań, samojezdnych samochodów, inteligentnych budynków i ulic będą wspomagane przez sieć. Zwiększenie różnorodności stosowanych czujników na brzegu sieci będzie zwiększała ilość danych i potencjalnie pożytecznych informacji. To z kolei powinno zwiększyć nasze bezpieczeństwo, poprawić jakość życia. W globalnym IoT wszystko wydaje się być powiązane ze wszystkim, także w swojej wzrastającej ilości i różnorodności. IoT dzisiaj ciągle odnajdujący, budujący i systematyzujący swoje atrybuty jest obecnie pełen przeciwstawności, pełen walki, współzawodnictwa a potem czasami jakiejś ugody, nawet pewnej konwergencji pomiędzy przeciwieństwami. Dywersyfikacja walczy ze standaryzacją, wirtualizacja z rzeczywistością, inteligencja naturalna ze sztuczną, prostota ze skomplikowaniem, jakość danych z ilością, bezpieczeństwo z powszechną dostępnością i mobilnością, niezawodność z kosztami, konwergencja i remediacja z indywidualizacją, nauka ludzka z automatycznym maszynowym odkrywaniem wiedzy, szybkie życie wspomagane IoT

z życiem wolnym naturalnym, duma człowieka z potencjalną przewagą w przyszłości maszyn zbudowanych przez człowieka, itp.

Przypadłości naszego życia o łącznej, potocznej nazwie różnorodność, czasami oczekiwanej i przyjemnej, czasami nadmiernej i dokuczliwej, nie leczy się lekarstwem monokultury. Tam gdzie chodzi o duży przerób i uzysk stosuje się monokulturę, ale tylko tam. I chroni się ją specjalnie bo jest bardziej podatna na epidemie niż różnorodność. IoT staje się częścią naszego życia. IoT będzie zawierał monokultury tam gdzie to potrzebne i ciągle zwiększającą się różnorodność gdzie indziej, podążającą za wiecznymi zmianami człowieka, jego potrzeb, zachcianek, marzeń, emocji, i jego otoczenia. Bezpośrednie otoczenie człowieka pozostawmy różnorodne, a tam gdzie to mniej widoczne, tam gdzie są osadzone fundamenty infrastruktury, stosujmy monokultury. Transmisja wielkich ilości danych IoT nie potrzebuje różnorodności. Dostarczanie danych człowiekowi, przetworzonych w informacje i wiedzę bezwzględnie wymaga różnorodności, ale w miarę możliwości jednak różnorodności jakoś uporządkowanej. Tutaj właśnie lokalizujemy te heroiczne i kosztowne wysiłki standaryzacyjne i normalizacyjne przez duże zespoły specjalistów w obszarze wszystkich warstw IoT. Patrząc na IoT ze znacznie większego dystansu, w sposób niemożliwy bo z zewnątrz naszego ekosystemu, jawi się on jako zwykła, wręcz trywialna konsekwencja projekcji inteligencji człowieka ma świat zewnętrzny. Jak to jeszcze możliwe aby ten świat zewnętrzny nie obdarzyć, jak najszybciej częściowo a potem coraz więcej, inteligencją współdziałającą z naszą własną wbudowaną, odziedziczoną za darmo, genetycznie, ewolucyjnie. Przecież wiemy jak i potrafimy to zrobić. To było łatwe do przewidzenia. A niemożliwe do przewidzenia, bo znajduje się być może częściowo poza naszym ekosystemem, jest czy to wyjdzie nam na dobre czy niekoniecznie. Czy budujemy cywilizację wolności i szczęśliwości, czy przeciwnie hodujemy Wielkiego Brata, powracając do epoki niewolnictwa. Albo coś pośredniego. Niezależnie od odpowiedzi na to pytanie wykonujemy obowiązkowy lot w przyszłość. W czasie lotu, czując nieodparty przymus, częściowo tylko zrozumiały imperatyw, napędzany genotypem i wolną wolą, a czasami szaleństwem lub przypadkiem, wymyślamy nowe narzędzia takie jak IoT porządkujące i usprawniające naszą pracę i otoczenie, pracowicie poszukujemy źródeł energii, chcemy lepiej zadbać i poprawić nasze zdrowie, zdobywać wiedzę o świecie, polepszać nasz byt tu i teraz, chcemy dominować, budować i burzyć, pędzić i zmieniać, zatrzymać się i pomyśleć, spojrzeć spokojnie z refleksją na świat, także przewidywać nieco lepiej niż obecnie co czeka nas za horyzontem przestrzeni, czasu, obecnych możliwości i wyobraźni, ultra horizonta.

Literatura

[1] Acharjya D.P., Geetha M.K. (2017), *Internet of Things: novel advances and envisioned applications*, Springer.
[2] Adams M. (2016), *Data analytics: using big data for business to increase profits and create happy customers*, Amazon Digital.
[3] Aiken M. (2016), *The Cyber Effect: A pioneering cyberpsychologist explains how human behaviour changes online*, John Murray.
[4] Alam M., Prasad N.R. (2017), *The rise of Internet of Things*, Amazon Digital.
[5] Angelakis V., Tragos E., Pohls H.C. , i in. (2017), *Designing, developing, and facilitating smart cities: urban design to IoT solutions*, Springer.
[6] Anissimov M., M. (2015), *Our accelerating future: how superintelligence, nanotechnology, and transhumanism will transform the planet*, Zenit Books.
[7] Al-Fuquaha A., Guizani M., Mohhamadi M. i in. (2015), *Internet of Things: A survey on enabling technologies, protocols, and applications*, "IEEE Communications Surveys & Tutorials", z. 17, nr 4.
[8] Armstrong S. (2016), *Smarter than us: The rise of machine intelligence*, e-book, Amazon.
[9] Ashgar N.H. (2016), *Internet of Things architecture research app with MQTT protocol*, Lambert.
[10] Attrill S. (red.) (2015), *Cyberpsychology*, OUP Oxford.
[11] Bagha A., Madisetti V. (2014), *Internet of Things, A hands-on approach*, Lexington KY, USA.
[12] Balani N. (2016), *Enterprise IoT, A definitive handbook*, Amazon, USA.
[13] Balani N. (2015), *Cognitive IoT*, Naveenbalani e-book, USA.
[14] Barkai J. (2016), *The outcome economy: How the Industrial Internet of Things is transforming every business*, Amazon.
[15] Barrat J. (2013), *Our final invention*, Thomas Dunnee Books, New York.
[16] BBVA Innovation Centre (2016), *Internet of Things*, e-book, Amazon.
[17] Bassi A., Bauer M., Fiedler M, i in. (2013), *Anabling things to talk: designing IoT solutions with the IoT architectural reference model*, Springer.
[18] Batalla J.M., Mastorakis G., Mavromoustakias C., i in. (2016), *Beyond the Internet of Things: everything connected*, Springer.
[19] Behman F., Wu K. (2015), *Collaborative Internet of Things (C-IoT) for future smart connected life and business*, IEEE, Willey, Chichesrer, UK.
[20] Berglass A., Black W., Thalind S., i in. (2015), *When computers can think: The artificial intelligence singularity*, e-book, Amazon.
[21] Behmann F., Wu Kwok (2015), *Collaborative Internet of Things (C0IoT): for future smart connected life and business*, Wiley.
[22] Bhatt C., Dey N., Ashour A.S. (2017), *Internet of Things and big data technologies for next generation healthcare*, Springer.
[23] Bostrom N. (2014), *Superintelligence, paths, dangeres, strategies*, OUP Oxford.
[24] Brain M. (2015), *The second intelligent species: How humans will become as ireelevant as cockroaches*, BYG Publishing.
[25] Brooks T.T. (2017), *Cyber-assurance for the Internet of Things*, IEEE Press, Wiley.
[26] Burakowski W., Krawiec P. (red.) (2012), *Inżynieria Internetu Przyszłości*, OWPW, Warszawa.
[27] Buyya R., Dastjerdi A.V. (2016), *Internet of Things, principles and paradigms*, Elsevier, New York.
[28] Capgemini (2016), *The impact of the Internet of Things on financial services*, Raport Techniczny.
[29] Case A. (2015), *Calm technology: designing for billions of devices and the Internet of Things*, O'Reilly Media.
[30] Chace S. (2015), *Surviving AI, The promise and peril of artificial intelligence*, Three Cs Publishing.
[31] Chen M. (2017), *Easy as Raspberry Pi: A step by step beginner's guide to building your own Internet of Things with the Raspberry Pi model 3*, Amazon Digital.
[32] Chen S., Ma R., Chen H-H., Zheng H., i in. (2017), *Machine-to-machine communications in ultra-dense networks – a survey*, "IEEE Communications Surveys & Tutorials", z. 19, nr 99.
[33] Chin S., Weaver J. (2015), *Raspberry Pi with Java: programming the Internet of Things*, Oracle Press, McGraw Hill.
[34] Chishti S., Barberis J. (2016), *The FinTech book: the financial technology handbook for investors, entrepreneurs and visionaries*, Wiley.
[35] Chmielecka J. (2017), *Internet złych rzeczy*, Pacal.
[36] Chou T. (2016), *Precision: Principles, practices and solutions for the Internet of Things*,
[37] Connoly I., Palmer M., Barton H., I in. (2016), *An introduction to cyberpsychology*, Routledge.
[38] Covington D. (2015), *Analytics; Data science, data analysis and predictive analytics for business*, Amazon Digital.
[39] DaCosta F. (2013), *Rethinking the Internat of Things*, Apres Open, New York.
[40] Darnell L. (2016), *The Internet of Things: A look at real-world use cases and concerns*, e-book, Amazon.
[41] Delikato F.C., Pires P.F., Batista T. (2017), *Resource management for Internet of Things*, Springer.
[42] Delikato F.C., Pires P.F., Batista T. (2013), *Middleware solutions for the Internet of Things*, Springer.
[43] DelMonte L.A. (2016), *The artificial intelligence revolution: will artificial intelligence serve us or replace us?*, e-book, Amazon.
[44] Dennis A.K. (2015), *Raspberry Pi home automation with Arduino*, Packt Publishing.
[45] Dhanjani N. (2015), *Abusing the Internet of Things, blackouts, freakouts and stakeouts*, O'Reilly,
[46] DiFatta G., Fortino G., Li W., i in. (2015), *Internet and distributed computing systems*, Conference Proceedings IDCS 2015, Windsor UK, Springer.
[47] Doukas Ch. (2012), *Building Internet of Things with the Arduino*, Create Space Publisher.
[48] Eclipse.org (2016), *The three software stacks required for IoT architectures*, Technical Report.
[49] Elbaz L., Behan M. (2017), *Essentials of cybersecurity*, Amazon Digital.
[50] Erl T., Puttini R., Mahmood Z. (2013), *Cloud Computing: Concepts, technology and architectures*, Prentice Hall.
[51] Etter D. (2016), *IoT security: practical guide book*, CreateSpace.
[52] Etter D. (2017), *Internet of Things programming: A simple and easy way of learning IoT*, e-book, Amazon.
[53] Faihead H. (2016), *Raspberry Pi IoT in C*, I/O Press.
[54] Familiar B. (2016), *Microservices, IoT, and Asure: Leveraging DevOps and nix=croservics architecture to deliver SaaS solutions*, Apress.
[55] Fisher A. (2016), *IBM Watson cognitive IoT*, Raport Techniczny.
[56] Floerkemeier Ch., Langhainrich M., Fleisch E., I in. (2008), *The Internet of Things*, Proceedings of the First International Conference, IoT 2008, Zurich, Switzerland, Springer.
[57] Ford M. (2015), *The rise of the robots, Technology and the threat of mass unemployment*, Oneworld.
[58] Fortino G., Trunfio P. (2014), *Internet of Things based on smart objects: technology middleware and applications*, Springer.
[59] Foth M., Brynskov M., Ojala T. (2015), *Citizen's right to the digital city: urban interfaces, activism, and placemaking*, Springer.
[60] Fraden J. (2016), *Handbook of modern sensors: physics, designs, and applications*, Springer.
[61] Gilchrist A. (2016), *Industry 4.0, The Industrial Internet of Things*, Apress,
[62] Gilchrist A. (2017), *IoT security issues*, De|G Press.
[63] Greengard S. (2015), *The Internet of Things*, The MIT Press, Cambridge.

[64] Guerrieri A., Loscri V., Rovella A., i in. (2016), *Management of cyber physical objects in the future Internet of Things: methods, architectures and applications*, Springer.
[65] Guinard D., Trifa V. (2016), *Buiding the Web of Things: with examples in Node.js and Raspberry Pi*, Manning.
[66] Hartman K. (2014), *Make: wearable electronics: design, prototype, and wear your own interactive garments*, Maker Media.
[67] Holler J., Tsiatsis V., Mulligan C. i in. (2014), *From machine-to-machine to the Internet of Things: Introduction to a New Age of intelligence*, Academic Press, Amsterdam.
[68] Hu F. (red.) (2016), *Security and privacy in Internet of Things (IoTs), models, algorithms and implementations*, CRC Press, Taylor and Francis, New York, USA.
[69] IBM (2015), *Automotive 2025: Industry without borders*, Executive Report, Somers NY, USA.
[70] IIConsortium.org (2016), *The Industrial Internet of Things*, Technical Report.
[71] IIConsortium.org (2015), *Industrial Internet reference architecture*, Technical Report.
[72] Jackson H. (2016), *IoT opportunities: All you need for business success,* e-book, Amazon.
[73] Jamthe S. (2015), *The Internet of Things business primer*, Stanford Edition.
[74] Jamthe S. (2016), *IoT disruptions 2020: getting to the connected world of 2020 with deep learning IoT*, CreateSpace.
[75] Jaokar A.V. (2015), *IoT data science*, Sanford Edition.
[76] Javed A. (2016), *Building Arduino projects for the Internet of Things: experiments with real-world applications*, Apress.
[77] Jayakumar M. (2017), *The Internet of Things with esp8266 hands on approach: get started with Arduino IDE and ESP8266*, CreateSpace.
[78] Kellmereit D., Obodovski D. (2013), *The silent intelligence – The Internet of Things*, DnD Ventures, San Francisco.
[79] Kranz M. (2016), *Building the Internet of Things, Implement new business models, Disrupt competitors, Transform your industry*, Wiley, New York, USA.
[80] Kuhnel C. (2015), Building an IoT Node in less than 15$: NodeMCU&ESP8266, Skript Verlag Kuhnel.
[81] Kurniawan A. (2016), *Smart Internet of Things projects*, Packt.
[82] Leonhard G. (2016), *Technology vs. humanity, The coming clash between man and machine*, Fast Future Publishing.
[83] Liow W.Q. (2017), *Riding the waves of Internet of Things*, Amazon Digital.
[84] Li Shancang, Xu Da Li, Zhao, S. (2015), *The internet of things: a survey,* "Inf. Syst. Front." 17: 243-259. doi:10.1007/s10796-014-9492-7
[85] Li Shancang, Xu Da Li. (2017), *Securing the Internet of Things*, Syngress.
[86] Liyanage M., Gurtov A., Ylliattila M. (red.) (2015), *Software defined mobile networks: beyond LTE network architecture*, Wiley.
[87] Mach P., Becvar Z. (2017), *Mobile edge computing: a survey on architecture and computational offloading*, "IEEE Communications Surveys & Tutorials", z. 19, nr 99.
[88] Markakis E., Mastorakis G., Mavromoustakias C.X., i in. (2017), *Cloud and fog computing in 5G mobile network*, IET.
[89] Mavromoustakis C., Mastorakis G., Batalla J.M. (206), *Internet of Things (IoT) in 5G mobile technologies*, Springer.
[90] Mcaulay T. (2000), *RIoT control, understanding and managing risks and the Internet of Things*, Elsevier, Amsterdam.
[91] McEvan A., Cassimally H. (2014), *Designing the Internet of Things*, John Wiley, Chichester, United Kingdom.
[92] Miessler D. (2017), *The Real Internet of Things*, Amazon Digital.
[93] Miller M.R. (2015), *The Internet of Things: How smart TVs, smart cars, smart homes, and smart cities are changing the world*, QUE, Indianopolis IN, USA.
[94] Mougayar W. (2016), *The business blockchain: promise, practice, and application of the next Internet technology*, Wiley.
[95] Mukhopadhyay S.Ch. (2014), *Internet of Things: challenges and opportunities*, Springer.
[96] Nagpure A. (2016), *Internet of Things enabled*, e-book, Amazon.
[97] Olsson T. (2012), *Arduino wearables (Technology in action)*, Apress.
[98] Pailes-Friedman R. (2016), *Smart textiles for designers: inventing the future of fsabrics*, Laurence King Publishing.
[99] Pan A., Purushtthaman B. (2016), *IoT technical challenges and solutions*, Artech House.
[100] Palfrey J., Gasser U. (2013), *Born Digital, Understanding the first generation of digital natives*, Perseus Book Group, New York.
[101] Perera Ch., Zaslavsky A. Christen P. i in. (2014), *Context aware computing for the Internet of Things*, "IEEE Communications Surveys & Tutorials", z. 16, nr 1.
[102] Pfister C. (2011), *Getting started with the Internet of Things: connecting sensors and microcontrollere to the Cloud*, Maker Media.
[103] Prasad R., Dixit S. (2016), *Wireless world in 2050 and beyond: a window into the future*, Springer.
[104] PRPL Foundation (2016), *Security guidance for critical areas of embedded computing*, Technical Report.
[105] Pujolle G. (2015), *Software networks: virtualization, SDN, 5G, security*, Wiley.
[106] Rayes A., Salem S. (2016), *Internet of Things from hype to reality: the road to digitization*, Springer.
[107] Rodriguez J. (2015), *Fundamentals of 5G mobile networks*, Wiley.
[108] Rogers L., Stanfrod-Clark D. (2017), *Wiring the IoT: connecting hardware with Raspberry Pi, Node-Red, and MQTT*, O;Reiily Media.
[109] Romaniuk R.S. (2001), *Optyczny Internet terabitowy*, Komitet Elektroniki i Telekomunikacji PAN, Warszawa.
[110] Rossmann J. (2016), *The Amazon way on IoT, 10 principles for every leader from the worls's leading Internet of Things starategies*, Clyde Hill Publishing, USA
[111] Rowland C., Goodman E., Charlier M., i in. (2015), *Designing connected products: UX for the consumer Internet of Things*, O'Reilly Media.
[112] Ruparelia N.B. (2016), *Cloud Computing*, MIT Press.
[113] Russel B., Van Durren D. (2016), *Practical Internet of Things security*, PACKT Publishing.
[114] Santana G.A. (2013), *Data center virtualization fundamentals: understanding techniques and designs for highly efficient data centers with Cisco Nexus, UCS, MDS, and beyond*, Cisco Press.
[115] Sarver W. (2017), *The 5G deployment plan handbook: Vol.1, Technical deployment and history around building 5G and IoT businesses*, Amazon Digital.
[116] Sazonov E., Neuman M.R. (red.) (2014), *Wearable sensors: fundamentals, implementation and applications*, Academic Press.
[117] Schwartz M. (2016), *Internet of Things with ESP8266*, PACKT.
[118] Seta F., Sen J., Biswas A., i in. (red.) (2016), *From powerty, inequality to smart city*, Proceedings of the national Conference on Sustainable Built Environment, Springer.
[119] Shovic J.C. (2016), *Raspberry Pi IoT projects: prototyping experiments for makers*, Apress.
[120] Skinner Ch. (2016), *ValueWeb: how FinTech firms are using mobile and blockchain technologies to create Internet of Value*, Marshall cavendish International.
[121] Slama D., Puhlmann F., Morrish J. i inn. (2000), *Enterprise IoT, Strategies and best practices for connected products and services*, O'Reilly, USA.
[122] Smart J. (2014), *'Digital twins' could make decisions for us within 5 years* [online],
[123] www.news.com.au/technology/digital-twins-could-make-decisions-for-us-within-5-years-john-smart-says/news-story/72d-881779d5a137f4b9d38ab440512e9, dostęp 15.05.2017
[124] Smith J. (2016), *Data analytics: what every business must know about big data and data science*, Pinnacle Publishers.
[125] Smith S. (2017), *The Internet of Risky Things: Trusting the devices that surround us*, O'Reilly.
[126] Stackowiak R., Licht A., Mantha V., i in. (2015), *Big data and the Internet of Things: Enterprise information architecture for a new age*, Apress.
[127] Stankovic J.A. (2014), *Research directions for the Internet of Things*, "IEEE Internet of Thigs Journal", z.1, nr 1.
[128] Sterling B. (2014), *The epic struggle of the Internet of Things*, Strelka Press.
[129] Tapscott D., Tapscott A. (2016), *Blockchain revolution: how the technology behind bitcoin is changing money, business and the world*, Portfolio Penguin.
[130] Tervonen J., Isoherranen V., Heikilla M. (2015), *A review of the cognitive capabilities and data analysis issues of the future industrial Internet-of-Things*, 6th IEEE Conference "Cognitive Infocommunications".
[131] Thampi S.M., Bhargawa B., Atrey P.K. (2014), *Managing Trust in Cyberspace*, CRC Press, Taylor & Francis, Boca raton FL, USA.
[132] Uckelmann D., Harrison M., Michahelles F. (2011), *Architecting the Internet of Things*, Springer.
[133] Vermesan O., Friess P. (red.) (2014), *Internet of Things – from research and innovation to market deployment*, River Publishers.
[134] Vermesan O., Friess P. (red.) (2015), *Building the hyperconnected society: IoT research and innovation value chains, ecosystems and markets*, River Publishers.
[135] Vermesan O., Friess P. (2016), *Digitising the Industry; Internet of Things connecting the physical, digital and virtual worlds*, River Publishers.
[136] Vermesan O., Friess P. (red.) (2016), *Internet of Things – Global technological and societal trands*, River Publishers.
[137] Volkmann D. (2016), *The rise of digital twins* [online], www.linkedin.com/pulse/rise-digital-twins-dimitri-volkmann?trk=prof-post, dostęp 15.05.2017
[138] Waher P. (2015), *Learnig Internet of Things*, PACT.
[139] Womack D., Cave R., Foden M., i in. (2016), *Exploring the power of cognitive IoT, Generating timely action in oil and gas*, IBM Chemicals&Petroleum, Technical Report.
[140] Wu Q., Ding G., Xu Y., i in. (2014), *Cognitive Internet of Things: A new paradigm beyond connection*, arXiv:1403.2498 [cs.AI].
[141] Xu Li Da, He Wu, Li Shancang (2014), *Internet of Things in Industries*, "IEEE Transactions on Industrial Informatics", z. 10, nr 4.
[142] Zarko I.P., Broering A., Soursos S., i in. (2016), *Interoperability and open source solutions for the Internet of Things*, IoT 2016 Conference, Stuttgart, Springer.
[143] Zhang M., Qiu Y., Bai X., i in. (2015), *A novel architecture for Cognitive Internet of Things*, "International Journal of Security and Applications", z. 9, nr 9.
[144] Zhou H. (2012), *The Internet of Things in the Cloud, A middleware perspective*, CRC Press.