Środowisko, ludzie i czas jako czynniki rewolucji technicznej Internetu rzeczy

Wstęp

Wprowadzenie Internetu Rzeczy (IoT) powoduje ogromną zmianę w życiu człowieka. Często przedstawia się to w wyidealizowany sposób: wykorzystuje się najnowszą technologię, oprogramowanie jest wolne od błędów, urządzenia nigdy się nie psują, a użytkownicy są zawsze podekscytowani nowym cyfrowym życiem. Prawdziwe życie jest ewidentnie inne. Najpierw omawiane są główne czynniki, które wprowadzają zmiany i nieporządek do tego idealnego świata: środowisko, czas i ludzie. Środowisko może być agresywne. Współpracujące systemy żyją własnym życiem, a początkowa kompatybilność ulegnie pogorszeniu. Wsparcie systemów zniknie i wygaśnie. Utrzymanie ich w działaniu wymaga wysiłku, który po pewnym czasie może nie być dostępny. Projektowanie i wspieranie systemów IoT wymaga najlepszych specjalistów z unikalnym połączeniem umiejętności. Ponieważ są one rzadkie, wiele projektów będzie musiało zaakceptować przeciętne zespoły o ograniczonych możliwościach. Popychanie projektów i tak jest ryzykowne, ponieważ przeciętność w krytycznej infrastrukturze lub urządzeniach ratujących życie to droga do katastrofy. Cyberbezpieczeństwo to ważny problem. Systemy IoT są często niejednorodne, szybko ewoluują i zawierają komercyjne urządzenia z lukami w zabezpieczeniach. Ze względu na te trudne warunki zagwarantowanie trwałego bezpieczeństwa jest praktycznie niemożliwe. Ponieważ urządzenia i systemy IoT gromadzą i przetwarzają duże ilości danych, Big Data jest w tym kontekście gorącym tematem. Jednak mieszanie dowolnych danych w jakikolwiek sposób - o ile nie dokonuje się dzielenia przez zero - daje pewne rezultaty. Przy dobrej wizualizacji niebezpiecznie wyglądają jak prawda. Rozwój i zarządzanie adaptacyjnymi systemami uczenia się przypomina wychowywanie dzieci. Istnieje kompromis między uczeniem dobrych manier a umożliwieniem swobodnej adaptacji do świata zewnętrznego. Cyfrowe dzieci zyskują niezależność i mogą być trudne do kontrolowania przez swoich ludzkich rodziców. Urządzenia IoT obserwują świat i na nim działają. Już samo to rodzi liczne problemy etyczne. Taka inwazyjna, wszechobecna technologia nigdy nie jest neutralna. Oprócz wiedzy o tym, jak jest rozwijany, ważne jest, aby zapytać, dlaczego i dla kogo. Ta część dotyczy kilku aspektów IoT, które łatwo pominąć w czysto technicznej dyskusji, a mimo to są ważne.

Rewolucje techniczne

Kilka razy w historii ludzkości życie zmieniało się w sposób rewolucyjny. Za każdym razem pojawiał się jako coś nowego, nieporównywalnego z przeszłością. Czasami nowe wydarzenia były postrzegane jako końcowy etap rozwoju, jak koniec historii lub koniec nauki. Ale po każdym domniemanym wypowiedzeniu następuje kolejne zakłócenie. Zawsze dobrze jest spojrzeć w przeszłość, gdzie można rozpoznać wzorce podobne do obecnych, choć w innej scenerii.

Przeszłe doświadczenie

Za przeszłą rewolucję techniczną uważa się zazwyczaj rewolucję przemysłową - wynalezienie elektryczności lub komputerów. Jednak nawet znacznie wcześniejsze wynalazki miały dalekosiężne skutki, takie jak okiełznanie ognia czy wprowadzenie rolnictwa. Charakterystyczne właściwości rewolucji technicznej są następujące:

* Nawet jeśli ludzie widzą, że to nadchodzi, zakres zmian jest zaskakujący

* Konsekwencje są nieprzewidywalne

* Oznacza punkt bez powrotu

Poszczególne zmiany działają na połączony system, a reakcje można zaobserwować daleko od pierwotnej przyczyny. Rozważmy fazy przejścia od łowiectwa/zbieractwa do rolnictwa (rewolucja neolityczna). Wszystko zaczyna się od kobiety (mężczyźni polują), która zbiera kłosy dzikich traw do jedzenia.

* Kobieta konserwuje część ziaren i sieje je następnej wiosny

* Grupa jest właścicielem pola i nasion, majątek wymaga ochrony ←profesjonalni wojownicy

* Nadwyżka jest wymieniana zgodnie z zasadami ← liczby, pismo, prawo

* Jednostki większe muszą być zarządzane ← miasta, królowie i administracja

* Społeczność potrzebuje ideologii ← religia, literatura, monumentalna architektura

* Wybór ziarna ← bardziej produktywne gatunki

* Współpraca, a nie polowanie jako czynnik sukcesu ← adaptacja genetyczna

* Życie w wąskiej przestrzeni ←wymiana intelektualna, ale także rozprzestrzenianie się chorób zakaźnych

W ten sposób zachowanie garści ziaren – krok po kroku – zmieniło oblicze Ziemi. Niektóre są dobre, inne złe, inne neutralne. W każdym razie cywilizacja osiągnęła kolejny punkt bez powrotu. Dzięki rolnictwu ta sama ziemia mogłaby wyżywić populację 10 razy większą niż wcześniej. Dlatego myśliwi/zbieracze nigdy nie wygrają z rolnikami. Ceną jest to, że ludność uzależnia się od nowej technologii i powrót jest niemożliwy. Konsekwencje niepowodzenia są tragiczne. W XIX wieku zaopatrzenie Irlandii w żywność było uzależnione od ziemniaków. Podczas Wielkiego Głodu (1845–1852) choroba ziemniaka zniszczyła tę podstawową uprawę. Rozwiązaniem była masowa emigracja, która dała początek irlandzkiemu Bostonowi. Podobny ciąg wydarzeń oznaczał postępy rewolucji przemysłowej (od latającego wahadłowca na krośnie tkackim po brytyjskie parowce w zatoce Hongkongu) czy rewolucji komputerowej (od jednego ENIAC-a obsługiwanego przez komputerowych guru do iPhone'a w kieszeni każdego) . Każdy z nich dogłębnie zmienił styl życia i społeczeństwo. We wszystkich przypadkach zmiana zaczyna się od drobnego ulepszenia istniejących procesów. Kumulacja drobnych wydarzeń, poparta sprzyjającymi warunkami, prowadzi do zakłóceń. Rewolucja komputerowa skorzystała na tym, że dzięki właściwościom fizycznym materii i znacznemu wysiłkowi rozwojowemu, zgodnie z prawem Moore'a, efektywnie wzrosła gęstość elementów elektronicznych, przy podobnym wzroście pojemności pamięci masowych i łączy komunikacyjnych. Zakłada się wszechobecną obecność energii elektrycznej i dostępu do Internetu i rzadko rozważa się bezpieczną awarię, z wyjątkiem tak ograniczonych przypadków, jak drzwi przeciwpożarowe, które domyślnie muszą umożliwiać ucieczkę. Awaria kluczowego systemu informatycznego wyłącza część nieinformatyczną. Bez systemu kontroli lotu samoloty nie będą latać. Szpital zaatakowany przez wirusa ransomware nie wykona operacji. W obu przypadkach nadal możliwe są pewne ograniczone usługi, ale na bardzo ograniczoną skalę i obarczone wysokim ryzykiem.

Internet rzeczy jako rewolucja techniczna

Co nowego w IoT? Najwyraźniej drogę utorowało kilka wydarzeń. Rozprzestrzenianie się smartfonów mobilnych sprawiło, że wszechobecny sygnał bezprzewodowy stał się standardem. Tania moc obliczeniowa i pojemność pamięci umożliwiły przetwarzanie w chmurze. Nowe czujniki są mniejsze i tańsze, dlatego mogą być produkowane masowo i umieszczane wszędzie - na małych, ruchomych obiektach i na/w ludziach. Otwiera to drogę do praktycznie nieograniczonych możliwości zastosowania. Kilka dekad stopniowych zmian zmieniło ludzkie życie. W latach 60-tych, kiedy komputer

wymagał klimatyzowanego pomieszczenia ze wzmocnioną podłogą, pomysł oznaczenia torebki komputerem był nie do pomyślenia. Teraz można to zrobić za pomocą małych, chowanych urządzeń. To pokazuje, że technologia wykorzystywana później przez młodych ludzi będzie odnosić się do obecnej, jak iPhone do mainframe IBM 360. I dokładnie tak, jak w 1967 roku technologia 2017 była nie do pomyślenia, tak technologia 2077 (a nawet 2027) jest nie do pomyślenia teraz. To samo dotyczy aplikacji. W 1967 r. do opracowania rakiet (w FORTRAN) lub do wydrukowania listy płac (w COBOL) wykorzystano komputer. Umieszczanie śmiesznych filmów z kotami przez pojedyncze osoby i oglądanie ich na ręcznym urządzeniu przekraczało wyobraźnię. Podobnie można sobie wyobrazić pewne kierunki rozwoju na najbliższą przyszłość, ale daleko idące konsekwencje, zwłaszcza w życiu społecznym, są nieprzewidywalne. Kiedy około 1995 r. wolne pasmo telefonów komórkowych zostało wykorzystane do obsługi krótkich wiadomości SMS (SMS o długości 160 znaków), nikt nie był w stanie przewidzieć wpływu na życie społeczne, od randek do flashmobów, w których wiadomości mobilne pozwalają szybko i spontanicznie zgromadzić grupę ludzi. Istnieje kilka nowych obszarów zastosowań IoT: Przemysł 4.0 , śledzenie obiektów i logistyka, inteligentne miasta , telemedycyna, czujniki środowiskowe i inne. Ich bezpośredni cel jest wyraźnie widoczny, nie da się jednak przewidzieć ich długoterminowego wpływu na charakter i dynamikę interakcji społecznych, symbiozę człowiek-maszyna, niekontrolowaną ewolucję uczących się maszyn, czy podporządkowanie jednostek i społeczeństwa automatycznym algorytmom decyzyjnym . Eksperci zawsze starają się wypracować wizje przyszłości, ale prędzej czy później faktyczny rozwój się rozchodzi i pojawiają się nowe struktury społeczne i ludzkie zachowania.

Systemy cyber-fizyczno-społeczne

Samym celem systemów IoT jest intensywna interakcja ze światem fizycznym. Ten świat składa się z obiektów fizycznych, innych systemów technicznych i ludzi. Ludzie znów mają ciała fizyczne, działające zgodnie z naturalnymi prawami, oraz umysły, wspierające procesy umysłowe. Aby zbudować system współdziałający ze światem rzeczywistym, trzeba ten świat zrozumieć. Zostanie to omówione w tej sekcji. Rozważmy tutaj pozycję typowego programisty IoT z zapleczem IT. Jego/jej mentalność można podsumować w następujący uproszczony (i przerysowany) sposób:

*Obiekty mają stany binarne (0 lub 1) Zmiany między stanami są natychmiastowe

* Sprzęt można łatwo wymienić

* Oprogramowanie można łatwo zaktualizować i aktywować po zresetowaniu

* Ostatnie błędy zostaną znalezione w akcji

* Użytkownicy są jak programiści

Obiekty w świecie rzeczywistym są różne. Obiekty mają ciągłe spektrum stanów wielowymiarowych. Odpowiedź na pytanie „czy to urządzenie medyczne działa?” nie jest zwykłym „tak” lub „nie”. Obejmuje algorytm sterowania, wagę i natrętność, żywotność baterii, łatwy interfejs użytkownika, wskaźnik awaryjności oraz krótko- i długoterminową skuteczność.

Obiekty mają właściwości dynamiczne. Ogrzewanie dużego obiektu wymaga czasu i jest zgodne z równaniami różniczkowymi cząstkowymi w trzech wymiarach. Jeśli proces jest mierzony przez siatkę czujników rozmieszczonych w objętości kontrolowanego obiektu, deweloper musi mieć tego świadomość. Te właściwości dynamiczne mają składową proporcjonalną, całkową i różniczkową (PID), a jeśli sygnał sterujący nie jest odpowiedni (ma nieprawidłowy przebieg), obiekt może oscylować, stać się niestabilny i pęknąć.

Komputer po uaktualnieniu i zresetowaniu uruchamia się ponownie od zera. Jeśli pacjent ma wszczepiony defibrylator, należy go wymienić po awarii. Jednak po dłuższym użytkowaniu przewody prowadzące do serca są pokryte tkanką i ponowna operacja jest ryzykowna. Dla osoby starszej może to być śmiertelne. W przypadku urządzenia do wstrzykiwania płynów, jeśli substancja, dawkowanie lub czas były niewłaściwe, organizm potrzebuje trochę czasu na regenerację. Dlatego reakcja na zmodyfikowane ustawienia nie jest widoczna od razu. Oczywiście w przypadku zastosowań przemysłowych lub medycznych stopień bezpieczeństwa musi być wysoki i dobrze zdefiniowany. Postawa „najlepszego wysiłku" nie wystarczy. Należy określić łagodną degradację w przypadku częściowej awarii. Należy przeanalizować zachowanie, mentalność i preferencje rzeczywistych użytkowników. Zaczyna się od podstawowej ergonomii, takiej jak wielkość postaci, na przykład pacjenci z cukrzycą poddawani wstrząsowi insulinowemu mają ekstremalnie zmniejszoną zdolność widzenia. Operatorzy elektrowni jądrowej nie potrzebują grywalizacji w interfejsie użytkownika. Wszystkie te zagadnienia niekoniecznie są nauczane na kursach informatyki. Aby stworzyć niezawodne systemy oparte na IoT, potrzebna jest szersza perspektywa, zwłaszcza że konsekwencje działań podejmowanych przez system i podejmowanych przez jego oprogramowanie mogą być dość dotkliwe. Ta świadomość jest wymagana na każdym poziomie procesu rozwoju. Programista widzi swój kod w następujący sposób:

if (condition)

then action1

else action2

Program działa na prawdziwych ludziach. Akcją1 w kodzie może być ewakuacja lotniska, impuls defibrylatora, wezwanie karetki, zablokowanie karty kredytowej lub – w skrajnym przypadku – zastrzelenie drona. Dlatego programista musi być świadomy znaczenia kodu i odpowiednio określić i ocenić warunek. Inną pułapką są nieoczekiwane błędy występujące po akcjach programu (takie jak wyjątki w Javie). Powinny być obsługiwane prawidłowo, ale ponieważ zakłócają przepływ programu, programiści często po prostu rejestrują je w dzienniku lub wykonują obsługę pro forma. Zwłaszcza podczas pracy pod presją terminów, wielu kusiło mnie, by założyć, że taka sytuacja i tak nigdy nie nastąpi. Jeśli połączenie z bazą danych zostanie ustanowione lub plik zostanie otwarty, programista wie, że tam będzie. Ale czasami tak nie jest, a program zawiesza się w losowy sposób. W systemie IoT konsekwencją może być wyłączenie zasilania części miasta lub inny — w zależności od celu systemu. Dla programisty przyzwyczajonego do naciskania przycisku resetowania wymaga to zmiany mentalnej.

Środowisko

Środowisko, w którym działa system IoT, może być bardzo zróżnicowane. W zależności od jego zastosowania i wymaganego poziomu bezpieczeństwa należy określić i przetestować dopuszczalne warunki. Samolot pasażerski przelatuje przez turbulencje w fazie testów, ląduje z jednym silnikiem podczas burzy piaskowej i startuje przy -20 °C na oblodzonym lotnisku. Jest testowany z różnymi systemami lądowania według przyrządów, również w obecności zakłóceń elektromagnetycznych. Oczywiście nie wszystkie systemy muszą działać w równie trudnym środowisku - należy to dostosować do konkretnego przypadku. Taka procedura jest najnowocześniejsza w przypadku sprzętu o wysokiej niezawodności, któremu muszą towarzyszyć systemy IoT.

Środowisko fizyczne

System IoT jest początkowo opracowywany w dobrze kontrolowanych warunkach laboratoryjnych, ale środowisko, w którym zostanie wdrożony, może być dość trudne. Będzie wystawiony na działanie

zmiennej temperatury i wilgotności oraz wibracji. Problemy wewnętrzne to interakcja z innymi systemami, pola magnetyczne lub promieniowanie. Wyzwania na świeżym powietrzu obejmują warunki atmosferyczne, takie jak deszcz, śnieg, mróz lub przegrzanie. W niektórych strefach powszechne są huragany i tajfuny. W krajach o częstych aktywnościach sejsmicznych zachowanie podczas trzęsienia ziemi musi być dobrze zdefiniowane. Jeśli urządzenie nie znajduje się w chronionym obwodzie, może zostać skradzione lub fizycznie uszkodzone. Nawet w zasadniczo spokojnym kraju istnieje ryzyko skrajnego wandalizmu; na przykład ostatnio w Niemczech, gdzie podczas szczytu G20 w Hamburgu (7–8 sierpnia 2017 r.) bojownicy antyglobalistyczni przekonwertowali cytowane centrum do strefy wojennej w trzy noce. Podczas normalnej eksploatacji części materiałowe ulegają zużyciu. Powierzchnie czujników mogą się zabrudzić, co zniekształca pomiar. Rurki do iniekcji zapychają się i zmniejsza się ilość skutecznie wstrzykiwanej substancji. Potrzebują czyszczenia i wymiany. Podobno trzeba też brać pod uwagę błahe przypadki. Rozważmy czujniki infrastruktury umieszczone na szczycie pylonów mostowych. Ich mocowanie za pomocą śrub trwa dłużej i sprawia, że połączenie jest podatne na korozję. Przyklejone klejem mogą spaść i spowodować uszkodzenia. Te przykłady pokazują, że projektant musi wykazać się dobrą znajomością świata fizycznego, możliwych skutków (teraźniejszych i przyszłych) oraz posługiwania się wyobraźnią.

Inne systemy techniczne

System często zależy od dostępności i prawidłowego funkcjonowania innych systemów technicznych. W leczeniu chorób serca sygnały życiowe mogą być teraz stale monitorowane, a szpital może być automatycznie alarmowany w nagłych przypadkach. Z drugiej strony, typowa europejska toaleta restauracyjna znajduje się w piwnicy, osłonięta betonową podłogą i nie ma sygnału telefonicznego. Wąskie schody i złe powietrze zwiększają ryzyko niewydolności serca. System lokalny w zasadzie działa - wykrywa zdarzenie i generuje alarm - ale przepływ informacji jest zablokowany, więc akcja jest bezużyteczna. Projektanci powinni odpowiedzieć na pytania: Czy system powinien ostrzegać pacjenta o opuszczeniu strefy bezpieczeństwa? Czy zbyt wiele alarmów nie stanowi zagrożenia dla zdrowia? I ważny punkt: projektanci muszą być świadomi problemu. Kolejnym problemem jest możliwa interakcja. Systemy IoT są nowe i stosunkowo rzadkie, ale istnieją wizje przestrzeni wypełnionej komunikującymi się urządzeniami, z „inteligentnym pyłem" jako formą ekstremalną. Jeśli każdy projektant uważa swój system za jedynego właściciela przestrzeni fizycznej i przepustowości, może to prowadzić do kolizji. Np. może odbyć się spotkanie użytkowników systemów monitorowania serca - 100 osób w jednej sali. Czy będzie wystarczająca przepustowość i czy systemy nie będą przeszkadzać? Co więcej, wypełnienie przestrzeni urządzeniami IoT otwiera drzwi do złośliwych działań, ponieważ urządzenie podsłuchujące/atakujące jest małe i trudne do wykrycia. Jeśli wiele systemów konkuruje o oferowanie podobnej usługi, zakłócanie funkcji konkurenta jest kuszącą opcją. Wiele aplikacji opiera się na nawigacji GPS. Sygnał GPS jest dość słaby i łatwy do zacięcia. Celem ataku na GPS może być chęć wyłączenia nawigacji w określonym regionie, jak w przypadku północnokoreańskiego zagłuszania przestrzeni południowokoreańskiej . W niektórych miejscach, takich jak Kanał La Manche czy Cieśnina Malakka, istotnych dla handlu światowego, znaczenie strategiczne jest oczywiste. Obecnie w takich miejscach wdrażane są systemy backupu, takie jak eLORAN, rozbudowana wersja starszego LORAN-C. Ewidentnie przepływające statki muszą być wyposażone w kompatybilne urządzenia. Mogą być różne dla różnych lokalizacji, ponieważ zależą od lokalnych przepisów. Ten przykład pokazuje, jak podatna jest kompozycja niezależnych systemów. „Navigable" nie jest własnością samego statku, ale statku wraz z lokalizacją, czasem i aktualnymi warunkami. Podobnie, komunikujące się urządzenie medyczne nie jest samo w sobie funkcjonalne bez wspierającego środowiska, w którym jest bezużyteczne.

Czas

Systemy IoT są często obecne w ponadczasowej perspektywie. Jednak w przypadku szybko rozwijających się systemów czas odgrywa główną rolę.

Zmiana celów i wartości

Obecnie opracowywane systemy mają na celu rozwiązywanie bieżących problemów. Z biegiem czasu problem może zniknąć lub zostać przeformułowany. Zacznijmy od przykładu historycznego. Około 1900 r. w Paryżu administracja miasta została przytłoczona problemem śmieci wytwarzanych przez powozy konne. Wkrótce problem zniknął wraz z wagonami. Problem zagospodarowania siana i obornika został zastąpiony problemem zapewnienia miejsc parkingowych i zanieczyszczenia spalinami. Nowszym przykładem jest ewolucja telefonów publicznych. Dawno temu telefony były dostępne w biurach PTT (Post, Telegraph and Telephone). Następnie wdrożono budki publiczne, obsługiwane najpierw na pojedyncze monety, następnie ze skomplikowanym mechanicznym systemem płatności i wymiany, później zastąpione monetami i kartami chipowymi, a następnie kartami chipowymi. Żywotność każdego kolejnego systemu była krótsza. W pewnym okresie telefony publiczne były instalowane nawet w pociągach, restauracjach czy samochodach pierwszej klasy. Wraz z pojawieniem się telefonów komórkowych, większość telefonów publicznych została usunięta. Na każdym etapie system zbudowany w celu rozwiązania pewnego problemu był zastępowany innym, w coraz szybszym tempie. W przypadku masowo wdrożonego systemu każda wymiana wymaga wysiłku i może powodować marnotrawstwo. Można to uznać za oczywiste, ale płynne zmiany zależą od zdrowej ekonomii i możliwości technicznych. Jeśli te czynniki miasta ulegną degradacji i z czasem staną się interesujące jedynie jako stanowiska archeologii przemysłowej. W powyższych przykładach główny cel (transport, komunikacja) pozostał niezmieniony. Jednak ze względu na zmianę percepcji lub destrukcyjne wydarzenia, te cele również mogą się zmienić. Podróżowanie może stać się nieatrakcyjne z powodu terroryzmu. Masowe naruszenia prywatności i nadużycia danych mogą rozbić media społecznościowe i zatrzymać określone ilościowo programy. Złamanie publicznej kryptografii przez obliczenia kwantowe spowoduje wyłączenie wszystkich elektronicznych systemów płatności. To znowu zniszczy całą gospodarkę, jeśli w międzyczasie wyeliminowana zostanie fizyczna gotówka. Wreszcie, typowe nawyki mogą się zmienić – obliczanie czasu Ramadanu może stać się ważniejsze niż szybkie randki. O takich kwestiach wspomina się tylko po to, by podkreślić, że założenia o powszechnym stylu życia i obiektach pożądania nie są ani uniwersalne, ani stałe.

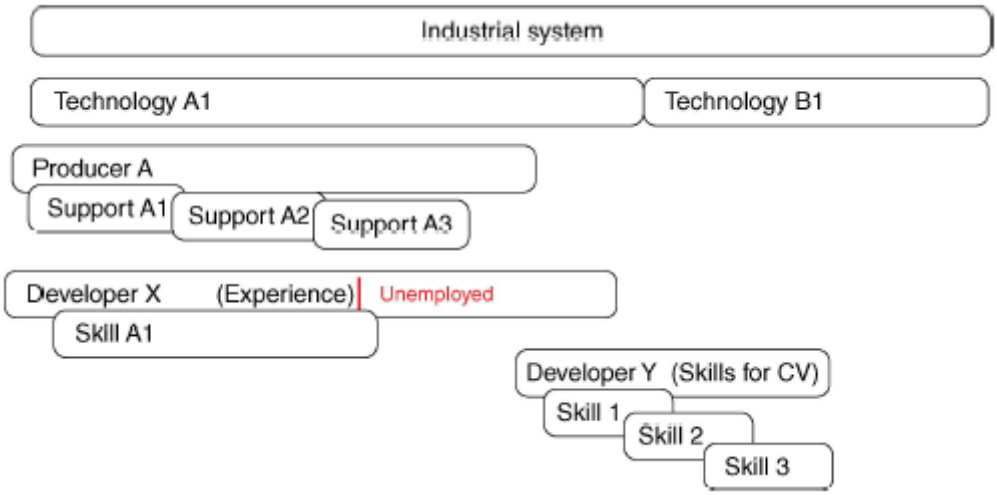
Degradacja interoperacyjności

Jak już wspomniano, system taki jak monitorowanie serca z automatycznym alarmem zależy od wielu innych systemów, których istnienie jest właśnie zakładane. Kontrolują je autonomiczne podmioty, takie jak szpitale ze służbami ratunkowymi, firmy telefoniczne czy operatorzy sieci energetycznych. Z niektórymi może być umowa o współpracy, z innymi nie. Po ustanowieniu takiego systemu istnieje ryzyko, że początkowa interoperacyjność z czasem ulegnie pogorszeniu. Społeczność naciska na nowe standardy, które zastąpią stare. Będą one realizowane przez poszczególne partie w wybranym przez siebie tempie. Nawet drobne modyfikacje protokołów komunikacyjnych lub definicji danych (np. kodowanie chorób) mogą mieć negatywne konsekwencje. Rzeczywisty problem zilustruje, jak pozornie błahe przyczyny mogą uniemożliwić współdziałanie. System IoT składa się z wielu komunikujących się urządzeń różnego typu. Na początku wszystko działa poprawnie. Integrator systemów kupuje urządzenia w dużych ilościach, producenci urządzeń kupują komponenty od zdalnych firm na podstawie aktualnej ceny. Po pewnym czasie podzespoły sprzedawane pod tą samą nazwą lub jako bezpośredni zamiennik wykazują niewielkie różnice w realizacji protokołu komunikacyjnego. Problem jest wykrywany tylko w instalacji klienta. Na rynku towarowym o niskiej marży niektórzy producenci są kuszeni na stosowanie fałszywych chipów. Może się zdarzyć, że producent oryginalnych chipów, który dostarcza również oprogramowanie sterujące, chce walczyć z nieuczciwą konkurencją. Automatycznie

aktualizowane oprogramowanie sterujące przestaje działać po wykryciu fałszywego chipa. Problem jest wykrywany jako awaria systemu końcowego i w zależności od poziomu ryzyka i poziomu bezpieczeństwa może mieć katastrofalne skutki, jeśli jest to samolot lub infrastruktura krytyczna pracująca nieprzerwanie. Problem jest nieoczekiwany, a jego pochodzenie jest na bardzo niskim poziomie. Koszt korekty może być ogromny, nawet przy założeniu, że producent podzespołu jest dostępny i gotowy do natychmiastowego działania. Po pewnym czasie ta firma może być zbankrutowana, zrestrukturyzowana lub nie mieć wystarczających zdolności i umiejętności, aby dokonać korekty.

Długoterminowa pomoc

Długotrwała eksploatacja systemu IoT napotyka na problem niekompatybilnych cykli życia powiązanego systemu przemysłowego, samego systemu IoT i zaangażowanych osób. Żywotność infrastruktury przemysłowej (elektrownie, koleje, mosty) mierzy się w dekadach. Będzie ewoluować - po tych samych torach jeździć będą szybsze pociągi, z ulepszonymi systemami sterowania, ale z zachowaniem ciągłości podstawowej konstrukcji. System sterowania, oparty pewnego dnia na IoT, mógł szybko ewoluować dzięki postępowi technologii. Jednak wielkość i ilość (setki stacji z wieloma rozjazdami, tysiące pociągów) sprawia, że modernizacja jest kosztowna i rzadka. Dlatego sprzęt żyje znacznie dłużej niż czas, w którym byłby używany do nowego projektu. Rozważmy system przemysłowy, który żyje przez dziesięciolecia, jak elektrownia.



Na początek zainstalowano komputerowy system sterowania wykorzystujący technologię A1. Dostarczył go producent A, który w międzyczasie wielokrotnie zmieniał linię produktów i być może dokonał fuzji, został przejęty lub wypadł z rynku. Uzyskanie wsparcia staje się z czasem coraz trudniejsze. Jeszcze gorzej jest w przypadku komercyjnych produktów gotowych (COTS), pochodzących z anonimowego źródła na Dalekim Wschodzie, gdzie dokumentacja jest skąpa, a wsparcie nie istnieje. Kiedy istniejąca technologia w końcu musi zostać zastąpiona przez obecny stan techniki (B1), ponownie konieczna jest dogłębna znajomość stanu obecnego. W tym momencie rolę odgrywają ludzie i ich umiejętności. Inżynierowie, którzy pracowali nad obecnym systemem, przeszli na emeryturę lub zostali zwolnieni. Ponieważ system rekrutacji koncentruje się na obszernej liście nowoczesnych umiejętności, inżynierowie są zachęcani do ich gromadzenia. Na przykład pozyskanie młodego profesjonalisty chcącego unowocześnić system przełączników elektromechanicznych z centralą zaprogramowaną w Visual Basic 4 jest prawie niemożliwe. Co więcej, jeśli firma nie jest doskonale zorganizowana, dokumentacja projektowa będzie niekompletna, z tekstami zapisanymi w WordPerfect na 5-calowych dyskietkach, co będzie jeszcze gorsze, jeśli rozwój zostanie zlecony na zewnątrz. Ten doskonały

przykład musi pokazać różnicę między światem idealnym a rzeczywistym. To, że opisuje przeszłość, nie powinno być pocieszeniem. Tylko rozpiętość czasu jest znacząca, a przyszłość będzie wyglądać tak samo, zwłaszcza przy jeszcze szybszym tempie postępów, zwinnym rozwoju i programistach często zmieniających pracę.

Erozja i gospodarka

Erozji podlegają wszystkie systemy techniczne (a także całkowicie naturalne formacje). Znana jest z poprzednich generacji technologii. Infrastruktura zainstalowana w mieście, taka jak sieć energetyczna, gazociągi, światłowody czy kolej podziemna, nie trwa wiecznie. Potrzebuje regularnej obsługi i okresowych aktualizacji, w przeciwnym razie rozpada się, pozostawiając w końcu tylko bezużyteczne relikty. Niedawnym przykładem takiego rozpadu może być Detroit, niegdyś rozwijające się miasto przemysłowe, a obecnie miejsce spektakularnych ruin. O problemie zaprzestania wsparcia i zapomnianych umiejętnościach wspomniano już wcześniej. Często milcząco zakłada się, że zapewnienie odpowiedniej obsługi zawsze będzie możliwe. W przypadku komputerów osobistych użytkownicy przyzwyczaili się do kupowania nowego, jeśli pojemność jest zbyt mała lub gdy coraz więcej programów przestaje działać poprawnie. W środowisku przemysłowym może to nie być rozwiązaniem. Liczba opracowanych systemów i ich indywidualny koszt mogą być zaporowe. Powoduje to pewną bezwładność. Ponadto modernizacja systemu przemysłowego przy zapewnieniu jego ciągłej pracy jest znacznie trudniejsza niż kopiowanie plików na nowy komputer. Jeśli na rynku nie będzie wystarczającej liczby zdolności i wykwalifikowanej kadry, system straci swoją funkcję. Program lotów księżycowych NASA może być ostrzeżeniem. Na przylądku Canaveral turyści mogą podziwiać ostatni pocisk Saturn V. W latach 70-tych, wspierany przez zdolny zespół, mógł polecieć na Księżyc. Teraz to tylko obiekt muzealny. Może się to zdarzyć w obecnych systemach, jeśli ludzie stracą zainteresowanie, wolę i zasoby. Istnieje ryzyko cyfrowego Detroit. Nie tylko pozostałości starych systemów nie będą działać, ale będą uciążliwe. To wystarczająco źle w przypadku instalacji przemysłowych, ale pacjenci mogą pozostać z niepodpartymi urządzeniami wszczepianymi w ich ciała. Rozpadający się materialnie i funkcjonalnie głęboki stymulator mózgu nie jest atrakcyjną opcją. Należy również wziąć pod uwagę bardziej ogólne kwestie. Przez wiele dziesięcioleci ludzie żyli w czasach prosperity, przynajmniej w świecie zachodnim, i zapomnieli, czym jest prawdziwy kryzys – katastrofą naturalną, kryzysem gospodarczym czy konfliktem zbrojnym. Oczywiście takie warunki będą miały katastrofalne skutki na każdym poziomie rozwoju technicznego. Takie możliwości kontrastują z częstymi wizjami nowego wspaniałego świata, w którym jedynym problemem będzie nadmiar wolnego czasu - i brak pracy dla 90% populacji.

Przenoszenie obiektów adaptowalnych

Inteligentne przedmioty dostosowują się do otoczenia i uczą się na doświadczeniu. Inteligentny dom wykrywa dzienne i tygodniowe rytmy i nawyki swoich mieszkańców. Zna również lokalne cykle pogodowe. Inteligentny samochód zna styl jazdy właściciela, jego życzenia i preferencje. Samochód bez kierowcy przyzwyczaja się do typowych tras, zwalnia przed szkołą i obserwuje, czy z fabryki wyjeżdżają duże ciężarówki. Wszystko działa idealnie, jeśli te rytmy są wystarczająco stabilne, a każde nowe wydarzenie raczej dodaje doświadczenie niż je niszczy. Każde urządzenie i system zachowuje się jak stary lokaj, znając pragnienia swojego pana, jeszcze zanim zostaną one wyrażone. Co się stanie, gdy zmienią się warunki? Czy rodzina powinna powiadomić o wyjeździe do domu, aby policja nie była wzywana w przypadku zmiany rytmu? Jeśli dostanie się tymczasowy mieszkaniec, na przykład użytkownik programu współdzielenia domu, takiego jak Airbnb, dom będzie musiał działać – zamknąć drzwi i zatrzymać intruza w środku. Gość zostanie uwolniony przez patrol policyjny pod warunkiem, że będzie posiadał elektroniczne dane uwierzytelniające do otwarcia drzwi. Jeśli w domu nie ma opcji dla tymczasowych mieszkańców, gość musi opuścić. W ten sam sposób dziadkowie mieszkający w domu

wyposażonym w system życia wspomaganego przez otoczenie nie mogą być odwiedzane przez wnuki bez przeprogramowania instalacji. Spersonalizowane obiekty i środowiska również muszą zarządzać własnością. Prawny właściciel posiada wszystkie certyfikaty tożsamości i klucze kryptograficzne, które pozwalają mu (i nikomu innemu) komunikować się z obiektem, odczytywać status i kontrolować go. Jeśli jest to obiekt/środowisko złożone z wielu elementów, jak np. inteligentny dom, muszą znać swoich sąsiadów, ponieważ będą wymieniać informacje tylko ze znanymi partnerami w sposób chroniony. Sprzedając inteligentny samochód, musi on zapomnieć o dużej części swoich doświadczeń. Nowy właściciel będzie miał inny styl jazdy i preferuje inne ustawienia (temperatura, pozycja siedzenia, stacje radiowe itp.). Będzie miał inny głos i będzie wyrażał polecenia innymi słowami. Ewentualnie zabierze samochód do regionu lub kraju o innym klimacie i gdzie inni kierowcy zachowują się inaczej. Jednak podstawowe umiejętności prowadzenia pojazdu - jak omijanie korków i przeszkód - nadal będą przydatne, choć zmieni się kształt i kolor przeszkody. Ponadto obiekt musi zostać przeniesiony w całości, łącznie ze wszystkimi prawami dostępu. W przeciwnym razie poprzedni właściciel zostanie z „zapasowymi kluczami". Tematy te są znane, choć w praktyce dominuje chęć sprzedaży samochodu lub domu i odłożenie problemów na później.

Ludzie

Technologię tworzą ludzie dla ludzi. Za układem sprzętowym stoi projektant, który zamawia układy scalone z katalogu tylko na podstawie ceny. Za systemem oprogramowania stoi programista, który pracuje pod presją czasu i nie ma czasu na analizowanie wszystkich pytań. Najwyraźniej przez większość czasu wykonują dobrą pracę, ale są zwykłymi ludźmi z mocnymi i słabymi stronami i osobistymi celami. Demografia jest również rzadko brana pod uwagę. Na przykład może być wymagane, aby wszystkie systemy wysokiego ryzyka otrzymały odpowiednią ochronę przed cyberatakami. Z liczby przyszłych systemów i wymaganych umiejętności technicznych - zakładając te wartości można oszacować - można wyprowadzić liczbę niezbędnych specjalistów ds. bezpieczeństwa z określonymi umiejętnościami. Ten prosty, liniowy model jest jednak błędny. Liczba ekspertów nie będzie rosła w nieskończoność; nasyci się (nieliniowość). Na przebieg procesu wpłynie sposób rekrutacji, przedkładający umiejętności nad doświadczenie. Wreszcie potencjalni eksperci ds. bezpieczeństwa, będący ludźmi, poszukującymi pieniędzy i szacunku, mogą być przyciągnięci przez inne zawody. W konsekwencji wiele przyszłych systemów nie będzie wystarczająco chronionych, niezależnie od wymagań.

Użytkownicy

Istnieje kilka klas użytkowników urządzeń i systemów IoT. Operatorzy instalacji przemysłowych przechodzą profesjonalne szkolenie, a korzystanie z tych systemów należy do ich obowiązków. Bardziej interesujący są użytkownicy indywidualni. Ich zachowanie to prawdziwy test konstrukcji urządzeń. Jeśli przenośne urządzenia będą rzucać się w oczy lub będą zbyt ciężkie, będą używane rzadko lub całkowicie odłożone. Interfejs użytkownika musi być dostosowany do zdolności poznawczych użytkowników, takich jak starsi pacjenci. Nie może pozostawiać miejsca na niejasności. Zdarzały się przypadki programowalnych pomp insulinowych, w których brak walidacji danych pozwolił na ustawienie dawki na szkodliwe dla zdrowia, prawdopodobnie śmiertelne wartości. Ręczne działanie jest również źródłem błędów. Jeśli pacjent musi umieścić łatkę czujnika na swojej skórze, lokalizacja może być niewłaściwa, a skóra może być zbyt sucha lub zbyt mokra. Ze względu na nieprzewidywalne zachowania użytkowników, należy zachować ostrożność przy analizie dostarczanych przez nich danych. Już podział użytkowników, którzy chcą korzystać z urządzenia i dzielić się danymi, powoduje stronniczość. Brakujące dane będą częstym problemem. Dane podane przez użytkownika, takie jak wiek, waga, wykształcenie itd., mogą być prawdziwe lub nie.

Deweloperzy

Jaki jest cel programisty? Chce mieć ciekawą, dobrze płatną pracę przez 40 lat, od 25 do 65 lat. W tym czasie zawód przechodzi kilka destrukcyjnych zmian. W przeszłości było to od taśmy dziurkowanej, dalekopisu i asemblera po smartfony i Javę. Ponieważ oczekuje się, że długość życia i wiek emerytalny będą podobne, można spodziewać się podobnej, jeśli nie szybszej, sekwencji zakłóceń. Działy zasobów ludzkich zwykle wybierają kandydatów zgodnie z listą umiejętności; niektóre firmy mogą zautomatyzować proces, zwłaszcza w początkowej fazie. Dlatego bogata kolekcja nowoczesnych buzzwordów daje przewagę na rynku. Wytrwałość, dotrzymywanie terminów, gotowość do wykonywania mniej spektakularnych zadań czy zrozumienie innych dyscyplin odgrywają drugorzędną rolę. Zarządzanie karierą w tworzeniu oprogramowania jest trudnym zadaniem, zwłaszcza podczas dużych zmian technologicznych. Co jest szczególnego w rozwoju systemów IoT? Nowością jest to, że tanie elementy pozwalają na szybkie wdrożenie urządzeń i systemów gotowych do masowego użytku. Z drugiej strony, poza systemami podobnymi do zabawek, mogą być wykorzystywane do odpowiedzialnych zadań, w których bezpieczeństwo ma kluczowe znaczenie. Na najwyższym poziomie istnieją inteligentne urządzenia medyczne, prawdopodobnie wszczepiane do organizmu, takie jak defibrylatory serca lub głębokie stymulatory mózgu. Nie tylko mierzą sygnały życiowe, ale działają bezpośrednio na organizm w podstawowych funkcjach. Najwyraźniej takich systemów nie mogą stworzyć młodzi programiści z doświadczeniem w lekkich aplikacjach na smartfony. Niezbędne jest dogłębne zrozumienie procesów fizycznych, chemicznych i biologicznych, a także dobra wyobraźnia, aby pomyśleć o możliwych zagrożeniach. Tacy programiści pracują dla firm przemysłowych, programując systemy sterowania dla pociągów, elektrowni i oddziałów intensywnej terapii. Najwyższym celem jest bezpieczeństwo i niezawodność. Często takie systemy ewoluują przez dziesięciolecia, wiedza domenowa jest niezbędna, a wszystkie narzędzia muszą być dobrze przetestowane przed użyciem. Użyteczność i przejrzysty dialog są kluczowe, atrakcyjność wizualna nie odgrywa żadnej roli, może być nawet niepokojąca. Druga społeczność to programiści „Cool Apps", znający wszystkie najnowsze narzędzia i chętni do ich zmiany co miesiąc. Żywotność ich produktów jest również znacznie krótsza; działają zatem w szybszej skali czasowej. Programowanie w świecie rzeczywistym jest do nich dodatkiem i często brakuje im wiedzy z zakresu nauk przyrodniczych. To jest stwierdzenie faktów, a nie krytyka. Tacy ludzie wnoszą innowacyjność niezbędną w szybko zmieniającym się świecie. Oba światy są dość oddzielone i istnieje między nimi niedopasowanie mentalności. Potrzebna jest równowaga między świeżością a doświadczeniem w zespole programistów. Jednak zdolna siła robocza może być ograniczeniem.

Zwolennicy

Wszystkie poważne systemy wymagają zorganizowanej konserwacji. W przypadku systemu heterogenicznego, współpracującego z innymi systemami, podstawowym pytaniem jest odpowiedzialność. Kto przejmuje kontrolę i gdzie są granice systemu? Systemy nie powinny być podzielone ziemią niczyją. Co się stanie, jeśli któryś ze współpracujących systemów zostanie zaktualizowany, z rozszerzoną lub nieznacznie zmienioną funkcjonalnością? Czy wszystkie zależności są znane i udokumentowane? Ewidentnie takie zadania wymagają dedykowanego, dobrze wyszkolonego personelu, posiadającego nie tylko ogólne umiejętności, ale także znającego szczegóły tej konkretnej aplikacji. Taką wiedzę można zdobyć tylko z czasem, a utrzymanie dobrych specjalistów nie jest łatwe. Specyficznym zadaniem jest zarządzanie bezpieczeństwem, niezbędne dla zapewnienia ciągłości działania. Zapotrzebowanie na wysoko wykwalifikowanych specjalistów stale rośnie. Takie umiejętności wydają się zapewniać optymalne perspektywy kariery w dającej się przewidzieć przyszłości. Temat jest jednak wymagający i istnieje różnica między formalnym certyfikatem a

doświadczeniem z życia wziętym. Brak ekspertów ds. bezpieczeństwa może być jedną z głównych przeszkód w rozprzestrzenianiu się bezpiecznych systemów IoT.

Menadżerowie projektu

Ponieważ projekty IoT są zazwyczaj multidyscyplinarne, jedną z ról kierownika projektu jest umożliwienie współpracy między osobami o różnych umiejętnościach, pochodzeniu, mentalności i nawykach. Przypadek inteligentnych urządzeń medycznych jest jednym z najtrudniejszych, ponieważ obowiązują surowe przepisy dotyczące bezpieczeństwa, a rynek jest trudny: urządzenie musi być „przepisane" przez lekarza i refundowane przez ubezpieczenia, w oparciu o dowód skuteczności. W związku z tym muszą współpracować: specjaliści od czujników biologicznych i aktuatorów (chemia, mikromechanika, nanotechnologia itp.); wiele klas programistów (oprogramowanie czasu rzeczywistego, aplikacje na smartfony, zabezpieczenia); specjaliści od Big Data, przetwarzania strumieniowego i analityki danych; statystycy; eksperci w procesach medycznych i szpitalnych, w procedurach zatwierdzania oraz w procedurach prawnych i etycznych, z poszanowaniem zasad prywatności; a może więcej. Oznacza to, że kierownik projektu musi być w stanie komunikować się z tak wieloma różnymi osobami i oczywiście mieć ogólny przegląd całości. Warto skorzystać z porad zewnętrznych ekspertów z innych dziedzin, którzy mogą wnieść inną perspektywę i pomóc wydobyć pominięte aspekty. Kolejnym ważnym zadaniem kierownika projektu jest utrzymanie zespołu, zwłaszcza w długoterminowym projekcie, który rozwija szereg powiązanych produktów z gwarantowanym wsparciem. Prowadzi to do gry z pracownikami, w której stawką jest stabilne zatrudnienie, sprzedające się umiejętności i długoterminowe perspektywy zawodowe. W tworzeniu oprogramowania istnieje kilka poziomów wiedzy i umiejętności. Podstawowy poziom to umiejętności informatyczne, takie jak znajomość języków i narzędzi. Następnym poziomem jest znajomość domeny, a następnie znajomość konkretnego projektu. Na otwartym rynku pracy decydujące znaczenie mają umiejętności informatyczne, które są w ciągłym ruchu. Wiedza domenowa jest atutem dla większych domen, takich jak bankowość, ale inwestowanie w wąskie domeny jest ryzykowne, ponieważ podlegają one silnym wahaniom. Doświadczenie w konkretnym projekcie nie jest żadnym atutem przy zmianie pracy. Z drugiej strony przy długotrwałym projekcie taki ekspert jest nieoceniony. Zna strukturę oprogramowania i zależności, dzięki czemu w przypadku prośby o modyfikację może natychmiast zareagować. Uzyskanie tego poziomu wiedzy zajmuje miesiące. Jednak gdy wsparcie produktowe jest wygaszane, taki programista, który przez lata pracował nad tym samym tematem i tkwił w tej samej technologii, ma bardzo złe szanse na rynku pracy, zwłaszcza jeśli nie jest jeszcze młody. Te wymagania definiują idealnego kierownika projektu, ale ewidentnie tacy ludzie są rzadkością. Grają w podobną grę jak ich pracownicy, ponieważ ciągłe zwiększanie wiedzy w dziedzinie, która pewnego dnia zaniknie, to ślepy zaułek. Pozytywną stroną jest to, że zarządzanie złożonymi projektami i praca z ludźmi to umiejętność zbywalna.

Producenci

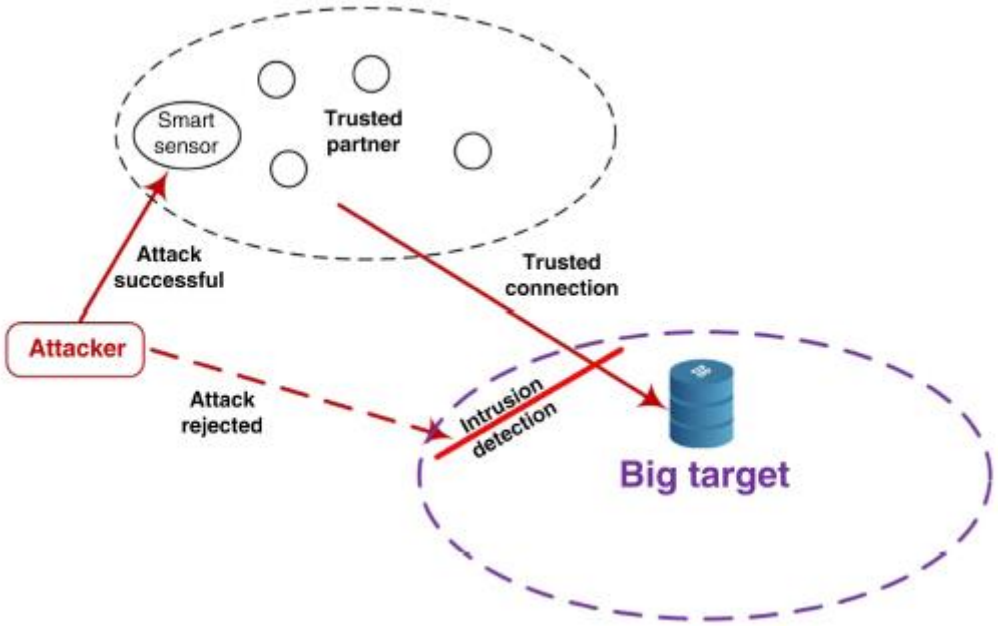
Producenci są zainteresowani produkcją, sprzedażą i osiąganiem zysków. Kierują się innowacjami i chcą być pierwszymi na rynku. Z drugiej strony obowiązują ich regulaminy określające bezpieczeństwo, ochronę danych osobowych oraz niezbędne badania i certyfikacje. Na przykład w przypadku produktów medycznych mogą być wymagane formalne badania kliniczne. W związku z tym znacznie więcej urządzeń (np. fitness trackery) jest sprzedawanych jako produkty komercyjne, dla których przydatność do poprawy zdrowia użytkownika jest sugerowana, ale nie jest formalnie udowodniona. Najwyraźniej jakość jest kluczowa dla firmy dotyczące reputacji i odpowiedzialności mogą być finansowo szkodliwe. Producenci chcą również rozwijać swoje produkty niskim kosztem. Odnosi się to do pytań, jak utrzymać optymalny zespół, jak zrównoważyć świeżość z doświadczeniem, czy rozwijać się lokalnie, czy zlecać na zewnątrz.

Regulatorzy

Regulatorzy dokonują przeglądu technologii i rynku oraz definiują i narzucają regulacje. Przed tymi zadaniami stoi wiele wyzwań. Istnieje wiele rynków z różnymi problemami. Samochody bez kierowcy mogą powodować wypadki, kamery monitorujące mogą naruszać prywatność, a urządzenia medyczne mogą szkodzić zdrowiu. Rynki te nie są rozdzielone, ponieważ technologie zostaną połączone: samochód bez kierowcy z kamerą na dachu może dokumentować podróż, ale także monitorować demonstracje polityczne lub szpiegować sąsiadów. Czy to samochód z kamerą czy kamerą z czterema kołami? Takie zacieranie się granic sprawia, że nie jest jasne, która instytucja jest faktycznie odpowiedzialna. Zwłaszcza w przepisach dotyczących prywatności granice kompetencji nie są ostre. Regulacje mają charakter krajowy lub regionalny, tak jak w Unii Europejskiej, ale Internet w zasadzie nie ma granic. Można kierować się zasadą, że żadne dane nie są wprost przekazywane do przetwarzania do innego państwa; jednak zagwarantowanie, że żaden pakiet danych nigdy nie przekroczy granicy państwa, jest praktycznie niemożliwe. Jeżeli francuska firma korzysta ze szwajcarskiego serwera (przypuszczalnie szczególnie bezpiecznego) i przechowuje dane klientów na całym świecie, to czyje zasady mają zastosowanie? Ponadto wszystkie zasady zabraniające ponownego wykorzystywania danych mają wyjątki, ponieważ dane te są niezbędne do utrzymania i doskonalenia usługi. Dane są formalnie własnością klientów, ale są zarządzane przez firmę, która ma pokusę, aby czerpać z nich jak najwięcej korzyści. Wreszcie podstawowym problemem jest dynamika rynku: ocena problemu, uwzględnienie wszystkich opinii i wykonanie testów wymaga czasu. Niektóre efekty widoczne są dopiero znacznie później, jak w przypadku zabiegów leczniczych. W międzyczasie problem może już nie mieć znaczenia. Odpowiedź już jest, ale pojawiają się nowe pytania. W ten sposób regulatorzy są naturalnymi przeciwnikami producentów, którzy postrzegają regulacje głównie jako przeszkody dla innowacji i inicjatywy. Oba stanowiska można bronić iw każdym przypadku konieczne jest wyważone porozumienie.

Bezpieczeństwo cybernetyczne

Urządzenie niepodłączone do sieci, nawet jeśli jest sterowane komputerowo, jest narażone na błędy oprogramowania i ma ograniczony zakres możliwych błędów. Tradycyjną infrastrukturę, taką jak elektrownia, można chronić, fizycznie kontrolując dostęp do obwodu za pomocą strażników, psów i reflektorów. Urządzenia i systemy sieciowe są dostępne na całym świecie i wymagają innego rodzaju ochrony. System IoT jest szczególnie wrażliwy, ponieważ do poszczególnych urządzeń można uzyskać dostęp bez fizycznego kontaktu. Wiele takich urządzeń jest kupowanych jako towar. W konsekwencji ich bezpieczeństwo zależy wyłącznie od producenta, któremu bardziej zależy na sprzedaży i przychodach. W urządzeniach sieciowych, takich jak kamery, wykryto wiele usterek, na przykład zakodowane dane uwierzytelniające, otwarte porty Telnet i klasyczne błędy, takie jak wstrzykiwanie poleceń SQL lub wykonywanie skryptów międzylokacyjnych. Niewłaściwie wykorzystywane przez złośliwych agentów mogą prowadzić do takich katastrof, jak atak DDoS (Distributed Denial of Service) przez botnet Mirai. Jak pokazano na rysunku, takie ukryte luki w zabezpieczeniach mogą się rozprzestrzeniać.



Jeśli złośliwe oprogramowanie przejmie kontrolę nad urządzeniem podłączonym do sieci, które jest widoczne z zewnątrz, może przejąć kontrolę nad serwerami systemowymi. Zależy to ewidentnie od szczegółów implementacji - jak dobra jest ochrona i jak sprytny jest atakujący. Właściciel tego systemu może nie docenić ryzyka ataku i zaoszczędzić na kosztach potrzebnych do właściwej ochrony. Ten peryferyjny system może nie być celem ataku, ale będąc zaufanym partnerem ważnej firmy, może służyć jako odskocznia i ułatwić pośredni atak na duży cel. Najwyraźniej zaatakowana firma może zwiększyć czułość swojego systemu wykrywania włamań, ale istnieje ryzyko zablokowania niezbędnego zaufanego połączenia przy każdym fałszywym zdarzeniu. W systemie sieciowym, który nie kontroluje wszystkich elementów i komunikuje się z kilkoma partnerami, taki margines zagrożenia będzie istniał. Oczywiście bezpieczeństwo elektrowni jądrowej nie może polegać na ustawieniu kamery w systemie partnera. System kontroli infrastruktury strategicznej musi być zbudowany w kręgach bezpieczeństwa, a wszystkie słabe punkty muszą zostać zidentyfikowane. Obecnie przewagę mają napastnicy, zwłaszcza sponsorowane przez państwo zespoły przeprowadzające ataki ukierunkowane, jak to (prawdopodobnie) miało miejsce w przypadku robaka Stuxnet, cyberataku na ukraińską sieć energetyczną w 2015 roku czy niedawnego robaka Petya, który zaatakował wiele firm przemysłowych, w tym Maersk, największą na świecie firmę żeglugową. Statków nie można było zadokować przez tydzień, a straty finansowe mają sięgnąć 300 milionów dolarów. System o wysokiej odpowiedzialności wymaga dogłębnej analizy zagrożeń i możliwości ich łagodzenia, dla których istnieją metody strukturalne. Istnieje kilka specjalnych przypadków, takich jak oprogramowanie urządzenia medycznego , w których występują problemy specyficzne dla domeny.

Rozumowanie z danych

Z zebranych danych można łatwo wygenerować statystyki i przedstawić je w atrakcyjnej wizualnie formie. Statystyka to jednak trudna dyscyplina, a droga od zbierania danych do uzyskania rzetelnej wiedzy jest trudna. Pierwszym problemem jest jakość danych. W Paryżu niedawno wdrożono system zanieczyszczenia mikrocząstkami. Czujniki umieszczane są na dachach samochodów należących do firmy dostarczającej energię elektryczną. Będąc tanim, mają mniejszą czułość. Co gorsza, brudzą się i wymagają ponownej kalibracji (lub czyszczenia). W związku z tym pokazują również trend zanieczyszczenia, ale wartości bezwzględne nie są wiarygodne. To pokazuje, że odczytywanie zmiennej zwanej „stężeniem cząstek" nie oznacza, że rzeczywiście zawiera ona wiarygodną wartość rzeczywistego stężenia cząstek. Należy sprawdzić, jak mierzona jest wartość, jaka jest precyzja i czy

warunki zmieniają się w czasie. Czy brakuje niektórych wartości, jak są traktowane? Jak dobrze znane są pozycje czujników? Kolejnym problemem jest stronniczość. W zastosowaniach medycznych wymagana jest zgoda na ponowne wykorzystanie danych. Projekty społecznościowe, takie jak skwantyfikowane self, opierają się na dobrowolnym udostępnianiu danych. Można się spodziewać, że zrobią to głównie młodzi, zaznajomieni z komputerami użytkownicy. Rozważmy system zbierania danych, który służy do pozyskiwania informacji o przebiegu niektórych schorzeń. Jeśli z tych danych wyciągnie się wnioski i odniesie się do całej populacji, osoby starsze będą traktowane jak osoby młode. Zazwyczaj interesujące są zależności przyczynowo-skutkowe, ponieważ można je wykorzystać do budowy modeli predykcyjnych. Wiele problemów opisuje złożona sieć współzależnych czynników. Jeśli wyszukiwanie wyników jest zbyt pochopne, istnieje ryzyko znalezienia fałszywych lub niepełnych korelacji. W przypadku medycznym rolę odgrywa wiele czynników. Szybkim rozwiązaniem jest wyodrębnienie tylko korelacji między bezpośrednio mierzalnymi wartościami (użycie urządzenia medycznego – sygnały życiowe), nie dlatego, że jest najważniejsza, ale dlatego, że jest najłatwiejsza w leczeniu. Jak głosi anegdota, niektórzy szukają zgubionego klucza pod latarnią, nie dlatego, że klucz tam wpadł, ale dlatego, że światło jest lepsze. W ten sposób inne ważne wpływy zostaną zignorowane, a wynikająca z tego reguła przyczynowości będzie miała ograniczoną wartość. Jednak identyfikacja wszystkich parametrów złożonego, ewoluującego systemu jest bardzo trudna. Wreszcie, często interesujące są długofalowe konsekwencje pewnych działań, takie jak wpływ leczenia lub wpływ środków bezpieczeństwa na przestępczość. Z drugiej strony wyniki są spodziewane szybko. Te wymagania są ze sobą sprzeczne. Dlatego przewidywania długoterminowe, oparte na obserwacjach krótkoterminowych, muszą być stale weryfikowane. Ponadto istnieje ryzyko, że dobrze przedstawione dane zostaną uznane za prawdziwe, właśnie ze względu na ich ilość i atrakcyjną prezentację. Jeśli są bezkrytycznie wykorzystywane do podejmowania decyzji (wiedza praktyczna), podejmowane działania mogą być błędne.

Adaptowalne systemy samoorganizujące się

W poprzednich rewolucjach technicznych ludzie wykorzystywali nowe sposoby wykorzystania właściwości materii w celu zmniejszenia wysiłku fizycznego, zazwyczaj bez większego żalu. Nikt nie biega za samochodami, nikt nie rywalizuje z wózkami widłowymi. Utratę mięśni rekompensowały ćwiczenia gimnastyczne wykonywane do woli. Wraz z rewolucją komputerową ludzie przenieśli proste umiejętności umysłowe na maszyny. W efekcie wielu straciło umiejętność czytania mapy i chcąc polecieć do St. Petersburga na Florydzie, może teraz wylądować w St. Petersburgu w Rosji. Wiele bardziej złożonych zadań zostało delegowanych, takich jak kontrola ruchu lotniczego, zarządzanie siecią energetyczną i tak dalej. Delegacja oznacza poleganie, a co za tym idzie zależność, bez odwrotu. Tymczasem nawet tak podstawowe zadanie sztucznej inteligencji (AI), jak gra w szachy, jest lepiej wykonywane przez maszynę. Sugeruje to, że ludzkość znajduje się na skraju przełomowej zmiany, w której ludzie są całkowicie uzależnieni od inteligentnej technologii, a rozwój tej technologii wymyka się spod kontroli. Pierwszy krok rzeczywiście się dokonał i niezbędne usługi zostały stopniowo delegowane na maszyny. Przyszłe scenariusze idą od stopniowej automatyzacji społeczeństwa do przejęcia przez sztuczną inteligencję przewyższającą ludzką. Coraz większa część ludzkiego życia jest kontrolowana przez algorytmy i dane. Algorytm uczący się dostosowuje się do obserwowanej rzeczywistości i sam się optymalizuje. Projektant definiuje początkowy algorytm i sposób uczenia się, ale wynik uczenia, czyli efektywny algorytm, zależy od danych i zmienia się dynamicznie. Ta ewolucja jest podobna do wychowywania dzieci: rodzice przygotowują swoje dzieci do samodzielności, ale nie chcą, aby przekraczały pewne granice i w razie potrzeby chcą interweniować. Na przykład handel narkotykami może wydawać się optymalnym rozwiązaniem problemów finansowych; jednak rodzice wiedzą, że jest to tylko lokalne, krótkoterminowe optimum. Algorytm decyzyjny niekoniecznie jest widoczny jako zwerbalizowane reguły. Może być raczej ukryta w wagach sygnału wielopoziomowej sieci neuronowej.

Dlatego na pewnym poziomie złożoności niemożliwe jest późniejsze podsumowanie rzeczywistych reguł lub ich modyfikacja, zwłaszcza jeśli sterowanie realizowane przez algorytm jest zbyt szybkie na ingerencję człowieka. Nawet jeśli projektanci zamierzają zbudować stosunkowo prostą pętlę sterowania, interakcje ze światem zewnętrznym – jeśli są wystarczająco silne – uczynią ją częścią złożonego, sieciowego systemu. Istnieją różne podejścia do teorii systemów. Ważną cechą takich systemów jest samoorganizacja i pojawianie się nowych właściwości na wyższym poziomie złożoności. Wyższy poziom jest oparty na niższym poziomie, ale nie jest przez niego w pełni wyjaśniony. Chemia opiera się na fizyce, a biologia na chemii. Chociaż DNA jest zbudowany z prostszych cząsteczek, te cząsteczki są zbudowane z atomów i atomów cząstek elementarnych; replikacji DNA lub produkcji białek nie można wyprowadzić z równania Schrödingera. DNA i białka są na nowym poziomie organizacyjnym, z własnymi właściwościami. Mówiąc prościej, złożony system to coś więcej niż suma jego elementów. Można się spodziewać, że w złożonych systemach uczenia się pojawią się nowe wzorce zachowań , zwłaszcza jeśli wiele oddzielnie zbudowanych systemów będzie współdziałać bez interwencji człowieka. Ludzie będą je obserwować, ale będą mieli na nie coraz mniejszy wpływ, jeśli w ogóle będą w stanie je zrozumieć. Szczególnym przypadkiem pojawiających się nieruchomości jest zachowanie roju lub inteligencja roju. Stado ptaków lub ławica ryb składa się z prostych elementów, które wchodzą w interakcje z sąsiadami według prostych zasad, jednak taka agregacja zachowuje się jak byt wyższego poziomu. Jest to powszechna właściwość takich systemów, niezależna od charakteru komponentów, dlatego należy ją zaobserwować w dużych systemach technicznych elementów adaptowalnych. Obserwowanie stad ptaków tańczących na niebie jest fascynujące, ale czy ludzie są gotowi cieszyć się samoorganizacją i zachowaniem roju swoich produktów? Oddanie kontroli w ograniczonym zakresie nie jest problematyczne. Pilot nie rozumie szczegółów sterowania powierzchniami sterowymi. Z drugiej strony automatyzacja całych miast, ich zasilania, ogrzewania, ruchu publicznego i prywatnego jest ryzykowna. W tym kontekście wykorzystanie IoT jest bardzo kuszące. Można zmierzyć czynniki środowiskowe, pozycje samochodów, wzorce ruchu człowieka i wiele innych. Inteligentne algorytmy zoptymalizują predefiniowane parametry. Różnorodne aktuatory będą sprawować władzę nad miastem. Nawet bez rozważenia złośliwego działania, pojawia się pytanie - czy to wszystko będzie działać na zawsze? Inteligentne miasta w broszurach wypełniają uśmiechnięte figurki Lego, radośnie cieszące się nowymi możliwościami. Jest to obraz mocno wyidealizowany. Wallach i Allen przedstawili spektakularny przykład małych przyczyn prowadzi do poważnych konsekwencji, z usterką rozprzestrzeniającą się między nie bezpośrednio połączonymi systemami: W upalny dzień cena spot ropy rośnie; elektrownie przechodzą na węgiel; eksploduje przeciążony generator węglowy; przeciążenia sieci energetycznej, szybko rozprzestrzeniają się przerwy w dostawie prądu; przerwy w dostawie prądu są identyfikowane jako działania terrorystyczne; lotniska są zamknięte, zderzają się lądujące samoloty. Ogólnie rzecz biorąc, wielu autorów ostrzega przed przedsięwzięciami zbyt złożonymi, aby można je było zrozumieć, zaprojektować, wdrożyć i utrzymywać. Sloman i Fernbach pokazują, jak przecenianie własnej wiedzy niemal prowadzi do katastrofy, jak w wybuchu termojądrowym w Castle Bravo w 1954 roku, gdzie bomba zaprojektowana na 6 M eksplodowała z siłą 15 M. W obliczeniach uwzględniono kilka czynników, ale pominięto je reakcja litu-7. Taleb ostrzega przed neomanią, dążeniem do kupowania lub wdrażania wszystkiego, co nowe, tylko dlatego, że jest to możliwe. Ostrzega również przed czarnymi łabędziami, rzadkimi zdarzeniami, które nie powinny mieć miejsca, ale czasami i tak się zdarzają. Jeśli system próbuje zbytnio kontrolować i nie ma wystarczającej elastyczności, takie czarne łabędzie mogą go poważnie uszkodzić, co może mieć nieprzewidywalne konsekwencje dla innych systemów technicznych i osób, które na nim polegają. W konsekwencji należy zadać sobie pytanie, jaki jest wymierny zysk systemu, jakie są zagrożenia (nawet niewiarygodne), jakie są środki bezpieczeństwa, jak będzie ewoluował i degradował i czy w ogóle trzeba go budować. Taleb w swojej wysoce godnej polecenia, otwierającej umysł książce klasyfikuje systemy ze względu na ich reakcję na zmianę: kruche (załamanie), solidne (opór) i

antykruche (ewolucja). W prawdziwym świecie, w którym tylko zmiana jest stała, systemy antykruche rozkwitają na dłuższą metę, na przykład życie lub zdecentralizowane organizacje polityczne. Ich ewolucja jest naturalnie niezależna i nieprzewidywalna i można zapytać, czy ludzie są gotowi zaakceptować równoległą ewolucję technologii, która wymyka się ludzkiej kontroli.

Rzeczy moralne

Wczesną wizję relacji między ludźmi a inteligentną technologią (w postaci humanoidalnych robotów lub innej) sformułował Isaac Asimov w jego opowiadaniu z 1942 r. „Runaround" jako Three Laws of Robotics. Asimov dodał później czwarte lub zerowe prawo, aby poprzedzić inne, jako bardziej ogólne:

0. Robot nie może skrzywdzić ludzkości lub przez bezczynność pozwolić ludzkości na krzywdę.

1. Robot nie może zranić człowieka ani przez bezczynność dopuścić do zranienia człowieka.

2. Robot musi być posłuszny rozkazom ludzi, z wyjątkiem sytuacji, w których rozkazy te byłyby sprzeczne z pierwszym prawem.

3. Robot musi chronić swoją egzystencję, o ile taka ochrona nie jest sprzeczna z pierwszym lub drugim prawem.

Główną wadą jest to, że ludzkość jest traktowana jako jednolita jednostka. W realnym świecie maszyny poszerzają możliwości różnych ludzi, mając różne, często rozbieżne lub sprzeczne cele. W łagodnej wersji nasze boty giełdowe konkurują ze swoimi botami giełdowymi. W skrajnym przypadku nasi wojownicy robotów walczą ze swoimi wojownikami robotów. Ludzie czasami mają tendencję do idealizowania technologii przyszłości (a czasami do demonizowania jej). Radio było już postrzegane jako ogólnoświatowe medium komunikacyjne, ułatwiające zrozumienie między narodami. Właściwie wkrótce został wykorzystany jako bezwzględna machina propagandowa. Ostatnio wielu postrzegało Internet jako oazę wolności, w której anonimowość pozwoli na swobodne wyrażanie opinii. Popularna kreskówka mówi: „W Internecie nikt nie wie, że jesteś psem". Teraz użytkownicy nie tylko nie są anonimowi, znane są również ich relacje, sytuacja finansowa, poglądy polityczne i orientacja seksualna. Dopóki te informacje są wykorzystywane tylko do sugerowania książek i filmów, są one nieszkodliwe, ale następny krok jest bliski - osoba, która jest anonimowa i szyfruje swoją komunikację, często używa jej do handlu narkotykami, fałszywymi paszportami i bronią lub do przygotowywanie ataków terrorystycznych. Swoboda wypowiedzi jest zdominowana przez obelgi ze strony innych ludzi i fałszywe posty przez sztuczne boty. Melvin Kranzberg powiedział: „Technologia nie jest ani dobra, ani zła; nie jest też neutralny". Może służyć zarówno do dobrych celów, jak i do złych, a samo jego istnienie przemienia świat. Wallach i Allen obszernie omówili temat etyki maszyn. Twierdzą, że ponieważ roboty biorą na siebie coraz większą odpowiedzialność, muszą być zaprogramowane z moralnymi zdolnościami podejmowania decyzji. Autorzy badają wyzwania związane z budowaniem sztucznych agentów moralnych, które rozszerzają ludzkie podejmowanie decyzji i etykę. Z technicznego punktu widzenia wyzwaniem jest zaszyfrowanie zasad etycznych, ich wdrożenie oraz zarządzanie nimi pozwalające na weryfikację i modyfikację. IoT znacznie rozszerza zakres wyzwań etycznych. Pozwala monitorować/inwigilować na niespotykaną dotąd skalę, a także masowo działać na przedmioty i ludzi. W zasadzie wszystkie informacje są gromadzone dla dobra ludzi. Posiadanie szczegółowych informacji o mieście pozwala na optymalizację zużycia energii i transportu publicznego. Jak zwykle przy dużej ilości informacji istnieje możliwość nadużycia. Rzeczy i osoby można śledzić elektronicznie. Kamery monitorujące mogą rozpoznawać twarze i tablice rejestracyjne samochodów. Będzie to uważane za dobre, jeśli zostanie użyte do łapania przestępców i terrorystów, ale jaka jest gwarancja, że nigdy nie zostanie wykorzystany do ucisku, gdy technologia zostanie wdrożona? Inny przypadek: Obserwacja osób starszych w domu pozwala wezwać pomoc w nagłych wypadkach. Ale kogo należy poinformować

i na jakich warunkach? Czy zmieniony wzorzec zachowania to tylko trochę wolności osobistej, którą należy szanować? Prawidłowe zachowanie obywateli może być monitorowane i doskonalone przez państwo niań dla ich własnego dobra. Nowy czujnik mierzy skład krwi i wykrywa ślady nikotyny i innych substancji. Niektórzy niepalący zgadzają się na wszczepienie takich urządzeń, aby płacić niższe składki ubezpieczeniowe. Wraz ze wzrostem użycia analizatorów krwi stają się one tańsze. Ponieważ palenie uważane jest za szkodliwe dla własnego zdrowia, a co za tym idzie dla społeczeństwa, rośnie presja na przymusowe używanie. Właściwe prawo jest uchwalone. Ten scenariusz jest realistyczny – w podobny sposób znakowanie psów chipem stało się obowiązkiem, a niewykonanie badań prenatalnych jest uważane za aspołeczne. Co może się wydarzyć dalej? Technologia jest wykorzystywana w innych kulturach do wykrywania spożycia narkotyków i alkoholu, z natychmiastowym powiadomieniem i surową karą. Wszystkie te opcje są zawarte w technologii, a reszta zależy od ludzkich decyzji.

Wniosek

IoT otwiera ogromny obszar dla kreatywnych zastosowań, które zmienią świat i ludzkie życie. Małe urządzenia wykrywające i działające, podłączone do Internetu, umożliwią prawdziwie wszechobecne przetwarzanie. Wsparcie dużych baz danych, analityki Big Data i algorytmów uczących umożliwi budowanie precyzyjnych modeli świata i rozproszonego środowiska AI, optymalizując życie ludzi i zachowując ich ekosystem. Każda praca jest idealnie dobra w idealnym świecie, jak już opisałem. Jednak w prawdziwym życiu baterie się rozładowują, rozmieszczone czujniki są skradzione lub wandalizowane, a sygnał bezprzewodowy brakuje. Systemy interoperacyjne na papierze mają niewielkie różnice w implementacji. Utrzymanie systemów działających, zwłaszcza jeśli są one zależne od innych systemów niezależnych dostawców, wymaga stałego wsparcia, a niezbędny personel może nie być dostępny. Istnieje również podstawowy konflikt między najnowocześniejszą, szybko rozwijającą się technologią a dłuższym okresem eksploatacji, gwarantowanym wsparciem, bezpieczeństwem infrastruktury krytycznej oraz urządzeniami i systemami ratującymi życie. Spotykają się dwa światy o odmiennej tradycji i mentalności. Rozwiązanie tej rozbieżności wymaga rozszerzenia interdyscyplinarnych programów uniwersyteckich, szkolenia na temat rzeczywistych przypadków oraz promowania współpracy między osobami o różnych umiejętnościach, wieku i pochodzeniu. Podobnie jak w przypadku poprzednich rewolucji technicznych, nowa technologia, taka jak wszechobecne wykrywanie lub wdrożone sztuczne narządy, zmieni ludzkie życie i interakcje między ludźmi. Tak jak poprzednio, długofalowy wpływ jest nieprzewidywalny i przekracza wyobraźnię. Nawet retrospektywna ocena wpływu – czy była dobra czy zła, dla kogo – jest daleka od jasności. W każdym razie taki rozwój nastąpi. Nic nie może tego powstrzymać. Jednak eksperci wraz ze społeczeństwem powinni obserwować go krytycznym okiem i starać się kierować nim zgodnie z celami wyznaczonymi przez człowieka i jego zasadami etycznymi.