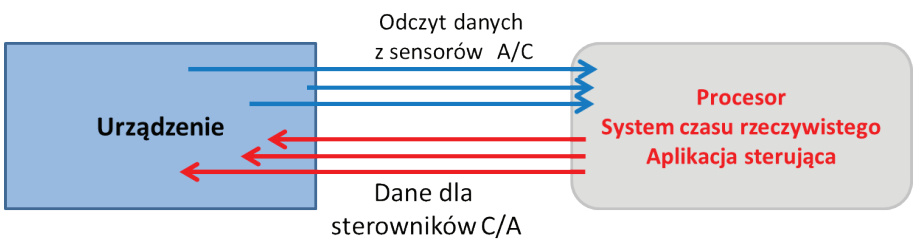
Rozdział 1
Internet of Things. Systemy wbudowane

§ 1. Najpierw były systemy wbudowane

Początkiem koncepcji dostępu i sterowania działaniem urządzeń poprzez Internet był (i jest) **system wbudowany** (ang. *embedded system*), którym jest procesor zarządzany systemem czasu rzeczywistego z dedykowaną aplikacją do sterowania urządzeniem (przedmiotem) na podstawie zbieranych z niego danych. Urządzenie z wbudowanym procesorem, systemem i aplikacją jest całkowicie autonomiczne. Zmiana reguł sterowania wymaga wymiany programu aplikacji.



Źródło: Opracowanie własne.

Tego typu rozwiązanie po raz pierwszy zostało zastosowane w kapsule Apollo w 1960 r. Od tego czasu jest już powszechnie stosowane np. w:

1) automatyce przemysłowej (robotach, obrabiarkach, tokarkach itd.);
2) w pojazdach (samochodach, ciężarówkach, pociągach, maszynach budowlanych itd.);
3) sterowaniu instalacjami chemicznymi, energetycznymi, jądrowymi itd.;
4) urządzeniach medycznych (tomografach, USG itd.);

5) urządzeniach codziennego użytku (pralkach, ekspresach do kawy, kuchenkach itd.).

Ponad 95% wszystkich wyprodukowanych, często specjalistycznych, procesorów jest wykorzystywanych w systemach wbudowanych!!!

Jeszcze niewiele z nich (szczególnie tych starszych) może być podłączonych obecnie do Internetu. Natomiast w nowszych egzemplarzach funkcja ta może być łatwo dodana.

§ 2. Przykłady

Jednym z najczęściej przywoływanych przykładów Internetu przedmiotów jest „inteligentny dom", w którym systemy oświetlenia, ogrzewania, klimatyzacji, ochrony oraz zarządzania wyposażeniem gospodarczym mogą być sterowane poprzez Internet. Jednakże jeszcze większość tego typu rozwiązań jest po prostu tylko zbiorem systemów wbudowanych – nawet gdy mogą być one sterowane z zewnątrz przez Internet z tabletu lub smartfona, gdyż z zewnątrz tylko zadajemy parametry działania wbudowanej tam aplikacji.

Drugim ciekawym przykładem jest „inteligentny samochód" z wieloma wbudowanymi systemami sterującymi poszczególnymi układami samochodu: silnikiem, skrzynią biegów, hamulcami, ochroną przed kolizją, klimatyzacją, drzwiami itp. Może to też czasem przysparzać kłopotów jego użytkownikowi, gdy (dla przykładu) automatyczne otwieranie i zamykanie z dociskaniem tylnej klapy jest sterowane przez system wbudowany. Wtedy ręczne zamykanie jest niedopuszczalne, gdyż nie zapewnia odpowiedniego zamknięcia klapy co powoduje konieczność zresetowania systemu!

W takich samochodach mamy już też systemy zbierające dane z zachowania się kierowcy (szybkość, bieg, położenie kierownicy, stan zapięcia pasów itp.) w ostatnich 30 sekundach, co może być wykorzystane przy analizach przyczyny wypadku.

W UE zdecydowano[1], że od października 2015 r. każdy nowy samochód ma być wyposażony w system *eCall* informujący automatycznie centralę ratowniczą o wypadku z przekazaniem podstawowych danych. Równocześnie producenci – jeszcze za zgodą użytkownika – oferują zdalne systemy diagnostyczne oraz serwisowe, informujące go o konieczności dokonania naprawy lub regulacji wskazanych układów.

O tym, że może to być już problemem dla ochrony danych osobowych, niech świadczy wypowiedź wiceprezesa *Jima Farleya* z Forda, przedstawiona w styczniu 2014 r. na Targach w Las Vegas – „We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing. By the way, we don't supply that data to anyone.".

[1] https://ec.europa.eu/digital-agenda/en/news/ecall-commission-recommendation-8-september-2011.

Co prawda, Ford wycofał się z tej wypowiedzi, ale takie możliwości techniczne już istnieją i będą niebawem powszechnie stosowane. W UE mówi się już o konieczności powszechnego instalowania w samochodach „czarnych skrzynek".

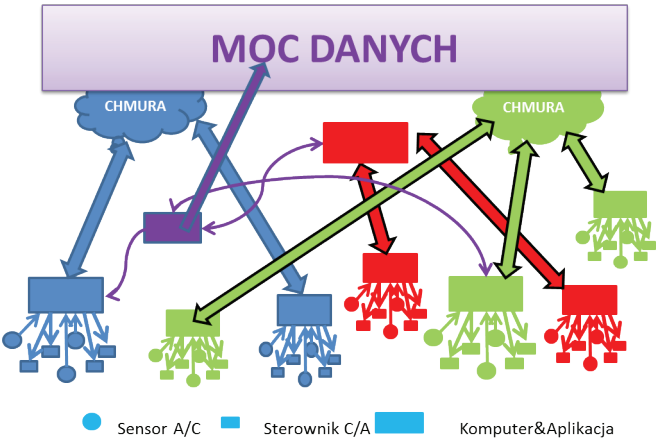
Innym ciekawym zastosowaniem, jeszcze niewykorzystywanym, może być zbieranie parametrów i zdarzeń z pokładu lecących samolotów i przekazywanie ich w czasie rzeczywistym do centrów danych. W sytuacjach awaryjnych, czy tuż po katastrofie nie byłoby konieczne poszukiwanie czarnych skrzynek. Nie wiem, dlaczego tego rozwiązania się nie stosuje – może tylko znaczna liczba lotów ogranicza możliwość wykorzystania tego pomysłu.

Źródło: Flightradar24.com.

§ 3. Korzystanie z Internetu przedmiotów

Pośród wielu przykładów realizacji Internetu przedmiotów omówimy podstawowy schemat jego działania.

Pojedyncze systemy (tutaj – czerwone, zielone i niebieskie) są początkowo systemami wbudowanymi. Następnie systemy czerwone są podłączone przez Internet do wspólnego systemu nimi zarządzającego – stają się Internetem czerwonych przedmiotów. Z kolei systemy niebieskie i zielone współdziałają poprzez aplikacje w chmurach. Obie chmury wraz z systemem fioletowym są scalone poprzez zbiór danych, którego analiza pozwala na dodatkowe sterowanie wybranymi systemami niebieskim i zielonym oraz czerwonymi.



Źródło: Opracowanie własne.

§ 4. Podsumowanie

Zastosowanie Internetu przedmiotów musi mieć sens i przynosić korzyści osobom i społeczeństwu, które może znajdować się w zasięgu ich działania. Wiele z pokazywanych aktualnie przykładów zastosowania kontrolowanych przez Internet przedmiotów jest mało przekonująca co do ich użyteczności. Często tylko niektórzy, szczególnie pozytywnie nastawieni na nowinki techniczne będą ich pierwszymi użytkownikami. Inni dopiero z czasem być może odnajdą sens w ich użytkowaniu.

Przez przedmioty podłączone do Internetu przekazywane są informacje o czasie i sposobie ich aktywności, ale też mogą być inne informacje, nawet niezwiązane bezpośrednio z zakresem ich działania. Już sam okres ich aktywności może być ważną daną osobową dotyczącą ich unikalnego (znanego z innych danych) użytkownika.

Dane (w tym dane prywatne) zbierane i przekazywane przez Internet przedmiotów mogą być „łatwo" przejęte i wykorzystane. Oczywiście pojęcie „łatwo" jest zależne od miejsca i sposobu ich połączenia z siecią oraz ich liczby w danym zastosowaniu. Zwykły, niezabezpieczony hasłem dostęp przez sieć Wi-Fi czy *Bluetooth*, będzie łatwo podatny na inwigilację, gdy połączenie siecią kablową z zabezpieczeniami już będzie wystarczającą ochroną.

„Darmowe" udostępnianie Internetu przedmiotów może być opłacane danymi z niego pozyskiwanymi. Obecnie istniejące modele finansowania udostępniania darmowego kontentu z reklam do niego dołączanych, będą mogły być zastosowane również dla Internetu przedmiotów, poprzez kolekcjonowanie danych mogących być następnie wykorzystanymi do ukierunkowanych personalnie reklam.

Nie istnieje (jeszcze) oprogramowanie w pełni zabezpieczające przed nieuprawnionym dostępem do przedmiotów podłączanych do Internetu. Jest to głównie spowodowane ogromną liczbą różnorodnych urządzeń wytwarzanych przez wielu producentów. Warto przy tym wiedzieć, że większość z tych urządzeń korzysta z uproszczonych protokołów dostępu do Internetu.

Nieuprawniony dostęp do przedmiotów podłączonych do Internetu może spowodować przejęcie kontroli nad przedmiotami przez niego sterowanymi, co może mieć negatywny wpływ zdrowotny, ekonomiczny lub psychiczny na osoby przebywające tamże. Problem tej ochrony przed nieuprawnionym dostępem do takich przedmiotów będzie krytyczny dla wielu zastosowań.

Przepisy prawne nigdy nie zabezpieczą w pełni osób i społeczeństwa przed nieuprawnionym, szkodliwym wykorzystaniem Internetu przedmiotów przeciwko nim. Problemem jest, w jaki sposób opisać ograniczenia prawne związane z funkcjonowaniem Internetu przedmiotów. Zapewne jeszcze nie możemy sobie wyobrazić wszystkich potencjalnych zagrożeń czy szkodliwych nieumyślnych oraz umyślnych działań wobec osób czy społeczeństwa. Czy należy je potraktować jako nową jakość, czy też może odnieść do już istniejących obiektów, takich jak komputery, telefony itp.? A może trzeba z każdym takim przedmiotem związać odpowiedzialność OC jego właściciela, gdy przedmiot, źle wysterowany, uczyni krzywdę (ostatnio robot w fabryce „zabił" robotnika[2]). Padają również pytania, kto będzie odpowiedzialny, gdy samochód – teraz to adekwatna nazwa tego przedmiotu – jadący samodzielnie spowoduje wypadek.

Zabezpieczenie interesów osób i społeczeństw korzystających z Internetu przedmiotów powinno być wmontowane technicznie w same przedmioty już na etapie ich projektowania. Takie założenie wydaje się naturalne, gdyż już obecnie wiele przedmiotów „samodzielnie" działających ma wbudowane elementy zabezpieczające ich użytkowników. Ale w wielu przypadkach nie znamy wszystkich możliwych szkodliwych działań dla wielu takich, dopiero projektowanych, przedmiotów i dopiero pierwsze awarie, wypadki czy wręcz katastrofy dadzą nam taką wiedzę – tak jak to się działo dotychczas. Będziemy musieli uczyć się na błędach – bo nasza techniczna wyobraźnia jest niewystarczająca.

Pełna wiedza o funkcjonalności każdego przedmiotu podłączonego do Internetu powinna być powszechnie dostępna w postaci zrozumiałej dla przeciętnie inteligentnej technicznie osoby. Chyba nie trzeba nikogo przekonywać, że powszechna obecność wokół nas inteligentnych przedmiotów sterowanych skądś i przez kogoś poprzez Internet nie może narażać obywateli

[2] http://www.telegraph.co.uk/news/worldnews/europe/germany/11712513/Robot-kills-man-at-Volkswagen-plant-in-Germany.html.

(w każdym wieku) na dyskomfort braku wiedzy, co do możliwego wpływu tych przedmiotów na ich codzienne życie. Stąd też pierwszym podstawowym prawem powinno być wymaganie pełnej informacji o możliwych skutkach działania (tylko może nie tak jak to jest obecnie przy lekach, gdzie jest klepana standardowa formułka, a ulotki zawierają ostrzeżenia typu, że jeden promil użytkujących dany lek może mieć „zgagę").

Nie są obecnie znane skutki społeczne i ekonomiczne gwałtownego powszechnego rozwoju zastosowań Internetu przedmiotów. Można to stwierdzenie traktować jako podsumowanie tej i innych dyskusji na ten temat. Wszyscy się dopiero uczymy, czym może być powszechne zastosowanie takich przedmiotów. Ale możemy już też stwierdzić, że – „Osoba, Społeczność, Społeczeństwo, Ludzkość musi być mentalnie, psychicznie, socjalnie i praktycznie przygotowana do obecności wokół siebie tysięcy przedmiotów podłączonych do Internetu oraz skutków z tego wynikających".

§ 5. Epilog

Jak wynika z podsumowania nie będzie łatwo ani inżynierom, ani użytkownikom – również tym przypadkowym i nie będzie łatwo prawnikom włożyć te nowe rozwiązania techniczne w przepisy prawne. Można mieć jedynie nadzieję, że młodsze pokolenia, zżyte już z kontentem Internetu oraz posługujące się sprawnie nowymi technicznymi rozwiązaniami poradzi sobie i z tymi problemami.

Tym bardziej że już szykuje się najmłodsze pokolenie – jeszcze będące w podstawówce – ze swoimi pomysłami na nowe zastosowania Internetu przedmiotów.

Przykładem niech będzie pomysł 7-letniej Natalii (oświadczam[3], że jest to praca całkowicie samodzielna), która zaprojektowała aplikację dla automatycznej szafy pakującej walizki na wyjazd. Najpierw przez Internet (wyszukiwarka *Google'a*) sprawdzana jest pogoda w docelowym miejscu wyjazdu, a potem na podstawie zapisanych w Pamięci preferencji są wybierane rzeczy do zapakowania. Aplikacja jest chroniona kodem: Pin 1_51_6.

[3] Zgodnie z art. 233 § 1 ustawy z 6.6.1997 r. – Kodeks karny (Dz.U. Nr 88, poz. 553 ze zm.).

Summary
Internet of Things. Embedded systems

The paper presents the source of the Internet of Things – the embedded systems, and then a few examples showing different aspects of this solution. After explaining the idea of the functioning of the IoT, the main threats for the protection of personal data and the possibility of their direct impact on the lives of people in their environment are indicated in the conclusion. It also describes the idea of the younger generation on the IoT application.