



PORTFOLIO:

Opracowanie analizy możliwości technicznych i funkcjonalnych integracji technologii Internetu Rzeczy w systemach automatyki budynkowej

Autorzy: Andrzej Ożadowicz, Jakub Grela

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl



1. Internet of Things – nowa koncepcja komunikacji sieciowej

Współczesny świat technologii komputerowych i sieciowych powszechnego użytku, to przede wszystkim niewielkie komputery osobiste – laptopy, notebooki, stacjonarne stacje PC, z dostępem do łącza sieci Internet. Jednak w ostatnich kilku latach, dzięki rozwojowi technologii mikroprocesorowych, wprowadzeniu na rynek telefonii komórkowej tzw. smartfonów, wzrostowi popularności portali społecznościach i mobilnych aplikacji dostępnych z poziomu tego typu urządzeń, sieci komputerowe, a w szczególności znana całej społeczności globalna sieć Internet, stają się popularnym, powszechnie używanym i uznawanym przez użytkowników środkiem wymiany informacji. Obserwowana tendencja do mobilności użytkowników sieci Internet (przenośne smartfony, tablety, notebooki), w połączeniu z wciąż rosnącą ofertą funkcjonalnych możliwości jej wykorzystania oraz dostępnych aplikacji, stały się zalążkiem idei połączenia w ramach sieci Internet różnych urządzeń, czujników, elementów wykonawczych.

Internet Rzeczy (Internet of Things - IoT) to koncepcja powszechnie przedstawiana jako kolejny etap komputerowej i sieciowej rewolucji, w kierunku rozproszenia modułów sieciowych i samych informacji, gdzie każdy obiekt w świecie rzeczywistym może automatycznie łączyć się z siecią, w pełni uczestniczyć w Internecie i komunikować się w dowolnym innym modulem do niej podłączonym. IoT obejmuje obecnie szereg technologii i obszarów badawczych, które mają na celu wykorzystanie i rozszerzenie istniejącej sieci Internet, jako platformy komunikacyjnej również dla różnego typu obiektów, urządzeń i modułów występujących w otoczeniu człowieka [1][2]. Dlatego też zmiana ulega obecnie tradycyjna koncepcja struktury i zasad funkcjonowania sieci Internet, rozumianej jako połączenia większych lub mniejszych serwerów danych z końcowymi terminalami klientów-użytkowników końcowych, w kierunku połączonych w sieci „inteligentnych” obiektów (Smart Object), wymieniających dane między sobą i w razie potrzeby lub żądanie, prowadzących interakcję z użytkownikami. Szczególnie istotny jest pierwszy z tych elementów, który wprowadza nową jakość i innowacyjność w struktury komunikacji w sieci Internet. Zakłada się bowiem możliwość dość znaczącej autonomiczności funkcjonowania obiektów sieciowych, które wymieniając między sobą informacje, uwzględniając zapisane algorytmy pracy, mogą realizować pewne działania oddziałujące na świat rzeczywisty, otoczenie, bez wiedzy i udziału użytkowników końcowych. To idea znana z branży automatyki przemysłowej i budynkowej pod hasłem Machine-to-Machine (M2M) i od wielu już lat realizowana w sieciach poziomu obiektowego, obsługujących czujniki i elementy wykonawcze w aplikacjach przemysłowych czy w budynkach. W ramach IoT staje się ona jednym z podstawowych elementów, jednak realizowanym już nie na poziomie obiektowym, ale przy założeniu wejścia w jednolitą, wysoce rozproszoną strukturę sieci protokołu IP. Koncepcja ich funkcjonowania musi opierać się zatem na trzech podstawowych założeniach: zdolności wzajemnej identyfikacji (każdy obiekt odnajduje i identyfikuje inne obiekty w sieci), komunikacji każdy z każdym (permanenta wymiana danych) oraz interakcji (wszystkie obiekty mogą ze sobą współpracować) [2][3].

2. Węzły sieci IoT – Smart Obiekty

Z punktu widzenia struktury połączeń sieciowych i organizacji sieci na różnych poziomach, Internet Rzeczy może być postrzegany jako wysoce rozproszona i dynamiczna w swej konstrukcji sieć transmisji danych, tworzona przez „inteligentne” moduły, węzły sieci tzw. Smart Obiekty, generujące i zarazem odbierające informacje. W branży i literaturze przedmiotu ustalono już uniwersalną definicję Smart Obiektu, jako jednostki o następujących cechach [1][2][3]:

- Posiada unikalny identyfikator/adres sieciowy
- Posiada prosty lub rozbudowany interfejs komunikacji z użytkownikiem/operatorem
- Posiada interfejs sieciowy i minimalny zestaw funkcji obsługujących komunikację – odbiór i wysyłanie komunikatów w przyjętym standardzie komunikacji, wraz z ich przetwarzaniem
- Ma możliwość komunikacji z innymi węzłami sieci – Smart Obiektami
- Ma możliwość pozyskiwania danych z otoczenia (czujniki), ich agregacji i przetwarzania oraz wywoływania akcji oddziałujących na otoczenie zewnętrzne (elementy wykonawcze)
- Posiada podstawowe funkcjonalności w zakresie przetwarzania danych cyfrowych
- Może podejmować decyzje co do własnego działania oraz współpracy z innymi węzłami sieci – Smart Obiektami

Interakcja z rzeczywistym światem zewnętrznym, osiągnięta jest poprzez implementację w strukturze sprzętowej Smart Obiektów odpowiednich czujników, których sygnały przetwarzane są w czasie rzeczywistym na pakiety danych oraz elementów wykonawczych, realizujących określone zadania, czynności, oddziałujące na środowisko zewnętrzne. Z kolei z perspektywy organizacji samych usług w oparciu o dane przesyłane między obiektami w sieci, wyzwaniem jest kwestia integracji, spójności danych oraz standaryzacji funkcjonalności. Dlatego konieczne jest zdefiniowanie standardów reprezentacji Smart Obiektów realizujących podobne funkcjonalności, w celu ograniczenia postępującej heterogeniczności struktur i elementów sieci oraz metod pozwalających na stosunkowo łatwą implementację Smart Obiektów w ramach konkretnych usług sieciowych, realizowanych zarówno na poziomie M2M, jak i przy interakcji z użytkownikiem [2]. Ze względu na fakt, iż węzły sieci – Smart Obiekty będą wykorzystywane w różnych aplikacjach, w pierwszym rzędzie można pokusić się o ich wstępne usystematyzowanie i podział na kilka grup, przy uwzględnieniu określonych wcześniej czynników. W jednym z badań [4], na podstawie doświadczeń przeprowadzonych głównie na aplikacjach przemysłowych, jako istotne czynniki kategoryzacji Smart Obiektów podano:

- „świadomość” – zdolność do postrzegania i interpretacji zdarzeń oraz aktywności osób w najbliższym otoczeniu zewnętrznym Smart Obiektu
- „reprezentacja” – aplikacja i jej model oraz środowisko i metody programowania Smart Obiektu
- „interakcja” – wymiana danych i informacji między Smart Obiektem a innymi węzłami w sieci lub z użytkownikiem/operatorem za pośrednictwem układów wej/wyj, sygnałów sterujących i sprzężeń zwrotnych

W efekcie zaproponowano trzy kategorie aplikacji Smart Obiektów, w różnym stopniu wykorzystujące przytoczone czynniki i związane z nimi funkcjonalności [4].

Pierwsza z nich to Smart Obiekty zorientowane na aktywność, a więc przede wszystkim wykrywające szybko zdarzenia jakie występują w ich otoczeniu i podejmujące autonomicznie działanie: rejestracja danych, wykonanie określonej akcji przez skojarzone z nimi elementy wykonawcze. Model aplikacji tego typu węzłów sieci IoT zawiera głównie funkcjonalności niezbędne do szybkiego gromadzenia dużych ilości danych i ich analizy, w celu generacji rozkazów dla elementów wykonawczych. Smart obiekty tej kategorii w zasadzie nie mają dedykowanych funkcjonalności do obsługi interakcji z użytkownikiem, ewentualnie w niewielkim zakresie z innymi węzłami sieci.

Kolejna kategoria to Smart Obiekty zorientowane na zachowanie wskazań, norm, ustalonych wartości itp. Ich struktura funkcjonalna bazuje na kategorii poprzedniej – aktywnej, jednak w połączeniu z interpretacją rejestrowanych sygnałów i danych z otoczenia i ich porównaniem z parametrami, nastawami, wartościami predefiniowanymi w algorytmie węzła sieci. W modelu aplikacyjnym zaimplementowane są zbiory zasad i ustawień, które w algorytmie działania służą do porównania danych gromadzonych przez węzeł sieciowy oraz ewentualnego podjęcia pożądanego działania, w celu zapewnienia zgodności z ustalonymi, predefiniowanymi dla danej aplikacji zasadami, parametrami. W zakresie interakcji dla tej kategorii węzłów sieciowych przewiduje się możliwość przekazywania informacji o zdarzeniach w których przekroczone zostały normy, ustalone parametry oraz monitoring określonych parametrów.

Trzecia z wyróżnionych kategorii to Smart Obiekty zorientowane procesowo. W ich algorytmach i aplikacjach uwzględnione są elementy dotyczące realizacji różnych zadań w obsługiwanym procesie bądź przemysłowym, bądź też dotyczącym sterowania wybranym elementem, podsystemem infrastruktury budynku, realizacją procesów monitorowania lub sterowania określonymi obiektami w otoczeniu węzła sieciowego lub użytkownika.

Proponowane algorytmy sterowania mają zwykle charakter kontekstowy, uwzględniają harmonogramy czasowe, sygnały przerwań od różnych czujników lub paneli/aplikacji zadających. W tego typu Smart Obiektach realizowana jest zwykle pełna interakcja z operatorem/użytkownikiem, zarówno w obszarze informowania go o zdarzeniach, zmianach parametrów procesowych, jak i reakcji na sygnały zdawane przez niego np. z mobilnych paneli sterujących itp.

Zaproponowane trzy kategorie aplikacyjne Smart Obiektów, stanowią pewną propozycję dotyczącą projektowania algorytmów i funkcjonalności węzłów sieci IoT. Proces projektowania aplikacji pojedynczych węzłów oraz ich wzajemnej integracji funkcjonalnej, powinien zawsze uwzględniać indywidualne aspekty charakterystyczne dla obsługiwanego procesu czy obiektu oraz wspomniane wcześniej trzy czynniki: „świadomość”, „reprezentację” i „interakcję”. Nie zawsze bowiem bardziej skomplikowany, abstrakcyjny i wielokontekstowy algorytm jest najlepszy. W wielu przypadkach prostsze rozwiązania i funkcje sprawdzają się lepiej i wpływają zarówno na szybkość działania aplikacji jak i jej niezawodność.

3. Technologie sieciowe i protokoły komunikacji

Praktyczna realizacja idei Internetu Rzeczy, o rozproszonej i zintegrowanej strukturze węzłów sieciowych i kanałów transmisji danych, opartych o protokół IP, wymaga również zmian w samym modelu tegoż protokołu. W strukturach istniejącej już i wciąż rozwijającej się globalnej sieci Internet pojawiło się bowiem widmo ograniczonych zasobów adresów sieciowych urządzeń serwerowych i klientów końcowych (protokół TCP/IP IPv4), które bazowały na słowach 32 bitowych. Opracowanie nowej wersji protokołu IPv6, gdzie podstawą adresów węzłów sieciowych (urządzeń w sieci) są słowa 128 bitowe, otworzyło nową perspektywę możliwości implementacji komunikacji z protokołem internetowym [5]. Staje się bowiem możliwe przypisanie konkretnego adresu IP do pojedynczych urządzeń: czujników, liczników, sterowników, modułów wykonawczych itp., które mogą stać się aktywnymi i równoprawnymi uczestnikami komunikacji sieciowej. W ten sposób możliwa jest i będzie organizacja ujednoczonego systemu wymiany danych bezpośrednio pomiędzy poszczególnymi węzłami sieci (tzw. Machine-to-Machine – M2M), bez udziału stacji nadrzędnych (np. serwery, stacje operatorskie) oraz w razie takiej konieczności lub żądania – przekazanie informacji operatorowi, systemom zarządzania, sterowania [1][2][3].

Wsparciem technologicznym dla rozwoju sieci IoT zwłaszcza na wspomnianym poziomie obiektowym, a zatem bezpośredniej obsługi dużej liczby czujników i elementów wykonawczych czy mobilnych urządzeń sterująco-monitorujących (np. tablet, smartfon), są również wszelkiego rodzaju technologie komunikacji bezprzewodowej, takie jak [6][7][8][9]:

- WiFi, sieć bezprzewodowa małego zasięgu. Możliwość łatwej komunikacji szczególnie z modułami mobilnej obsługi i sterowania (np. smartfony, tablety, laptopy). Dostęp do sieci Internet poprzez routery lub punkty dostępowe WiFi,
- Sieci komórkowe 2G, 3G i 4G. Możliwość komunikacji z dedykowanymi modułami GSM, UMTS, HSDPA, LTE z przyłączonymi do nich czujnikami lub urządzeniami wykonawczymi. Konieczne wyposażenie w kartę SIM oraz pozostawanie modułów w zasięgu sygnału sieci komórkowej,
- ZigBee, protokół dedykowany do sieci typu mesh w aplikacjach gdzie możliwe jest zastosowanie łączy o niskiej przepustowości. Standard ten zapewnia energooszczędność urządzeniom bateryjnym, przeznaczony do sieci, w której wymiana danych przebiega sporadycznie, okresowo,
- Z-Wave, również protokół bezprzewodowy dedykowany do systemów automatyki budynkowej, szczególnie do zdalnego kontrolowania urządzeń domowych lub oświetlenia, wykorzystuje sygnał radiowy niskiej mocy,
- 6LoWPAN (ang. IPv6 over Low Power Wireless Personal Area Networks), zwany również bezprzewodowym Internetem systemów wbudowanych. Zasadniczo jest to protokół IPv6 z pewnymi elementami pozwalającymi na jego bardziej efektywne wykorzystanie i implementacje w komunikacji bardzo małych urządzeń i czujników. Pozwala to na ich włączenie w strukturę Internetu Rzeczy – IoT,
- Bluetooth, protokół komunikacji bezprzewodowej dedykowany do łączenia modułów znajdujących się w niewielkich odległościach od siebie, charakteryzujący się stosunkowo dużą szybkością transmisji niewielkich pakietów danych.
- RFID, technologia wykorzystująca fale radiowe do transmisji niewielkich pakietów danych (zwykle identyfikator przedmiotu) wraz z zasilaniem samej etykiety RFID

zlokalizowanej na danym obiekcie. Możliwa jest identyfikacja wielu etykiet znajdujących się jednocześnie w polu odczytu.

Oprócz wymienionych technologii, poziom obiektowy systemów sieciowych to również od wielu już lat domena dedykowanych sieci obiektowych, zarówno przemysłowych jak i automatyki budynkowej. Instalacje automatyki bazujące na standardach takich sieci zaimplementowane są już w bardzo dużej liczbie obiektów, zapewniając obsługę czujników i urządzeń wykonawczych oraz realizując zaawansowane algorytmy i funkcje sterowania oraz monitoringu. Warto podkreślić, że podnoszone tak dobitnie w idei Internetu Rzeczy kwestie rozproszenia i integracji systemów wymiany danych między węzłami sieci, miały swój początek właśnie w tych rozwiązaniach technologicznych, obiektowych, ustandaryzowanych sieci automatyki. Dlatego też wielu dostawców urządzeń i technologii automatyki budynkowej i przemysłowej aktywnie uczestniczy obecnie w rozwoju platformy IoT. Docelowo przewiduje się również ograniczenie roli i znaczenia popularnych obecnie różnych standardów sieci obiektowych, obsługujących transmisję danych na najniższym poziomie, bezpośrednio obsługi np. czujników, modułów wykonawczych, koncentratorów danych, liczników itp., na rzecz właśnie tej jednolitej struktury sieciowej, z zaimplementowanym protokołem IPv6, jako uniwersalnym rozwiązaniem dla komunikacji między wszystkimi obiektami i węzłami sieciowymi [5].

4. Sieci IoT w automatyce budynkowej

Bez wątplenia różnego typu budynki (użyteczności publicznej, komercyjne, przemysłowe, biurowe i domy mieszkalne), wraz ze znajdującą się w nich infrastrukturą, urządzeniami AGD, RTV itp., są jednym z najważniejszych elementów otoczenia i środowiska życia współczesnego człowieka. Obiekty te powinny być rozpatrywane również w szerszej perspektywie, przede wszystkim ich bezpośredniego otoczenia (parkingi, place) oraz powstających obecnie koncepcji rozwojowych i technologicznych tzw. inteligentnych miast (Smart Cities). Budynki w takich strukturach organizacyjnych środowiska i otoczenia człowieka okazują się bowiem jednym z głównych konsumentów energii w różnych jej postaciach – elektryczna, ciepła, różne media.

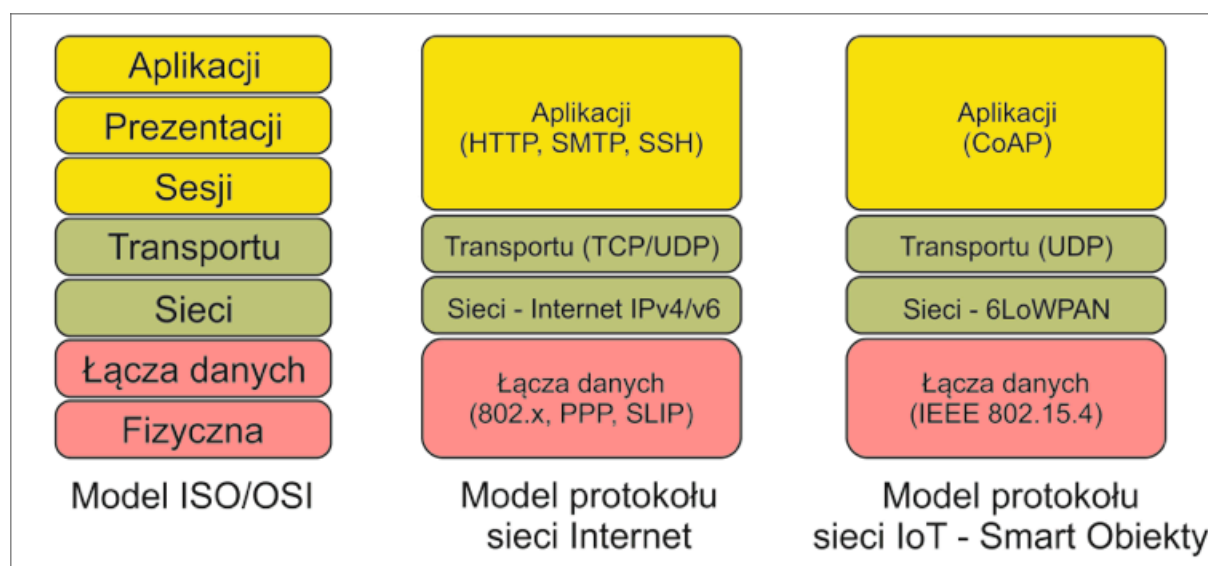
Zadania obsługi, zapewnienia komfortu i bezpieczeństwa w budynkach, monitoringu i sterowania urządzeń ich infrastruktury, kojarzone są dość powszechnie z systemami automatyki budynkowej (inteligentnych budynków – BAS – Building Automation Systems), realizowanymi w oparciu o różne standardy rozproszonych sieciowych systemów komunikacji: BACnet, LonWorks, KNX, ZigBee, M-Bus i inne. Standardy te, choć z reguły otwarte, nie zapewniają jednak możliwości interakcji między sobą, a więc bezpośredniego łączenia np. dwóch sieci wykonanych w różnych standardach. Związane z tym faktem wyzwanie dotyczące łączenia różnych infrastruktur sieci czujników i modułów wykonawczych oraz różnych technologii systemowych w ramach inteligentnych budynków i inteligentnych miast, podnoszone jest przez wielu specjalistów branżowych i naukowców [10]. Integracja taka musi uwzględniać dwa aspekty:

- wspomnianą już obsługę i włączenie do jednej platformy systemowej całych sieci magistralnych poziomu obiektowego różnych standardów, korzystających z dedykowanych magistral i mediów komunikacyjnych

- obsługę nowych urządzeń (czujniki, elementy wykonawcze, sterowniki itp.), działających jako indywidualne węzły sieciowe, z interfejsem IP, ale realizujące wspólne funkcje i zdania w systemie zarówno w komunikacji między sobą, jak i węzłami sieci zlokalizowanymi w ramach podsieci magistralowych.

Sieci obiektowe i Smart Obiekty

W branży współczesnych technologii automatyki budynkowej istnieje już kilka rozwiązań dedykowanych integracji danych z wykorzystaniem technik Internetowych i usług sieciowych Web, takich jak: oBIX, OPC UA czy BACnet/WS (WS-Web Service) oraz, coraz częściej implementowany interfejs RESTful WS, bazujący na standardowym protokole obsługi stron WWW - HTTP. Jednakże technologie to, choć popularne i sprawdzone w praktyce komunikacji sieci Internet w konfiguracji klient-serwer, stawiają dość wysokie wymagania sprzętowe węzłom sieci - w zakresie mocy obliczeniowej, pamięci i długości obsługiwanych pakietów danych. W celu umożliwienia implementacji protokołu IP w niewielkich urządzeniach (małe czujniki, elementy wykonawcze, jednocukładowe sterowniki czy moduły monitorujące), grupa robocza IETF (ang. Internet Engineering Task Force) w której uczestniczą m.in. przedstawiciele projektantów, operatorów i dostawców rozwiązań sieciowych, opracowała protokół aplikacji CoAP (ang. Constrained Application Protocol), dedykowany do aplikacji z węzłami sieciowymi o ograniczonych zasobach pamięci i mocy obliczeniowych, realizujących proste zdania i funkcjonalności, ale wymagających komunikacji za pośrednictwem sieci Ethernet lub Internet [10][11]. Protokół CoAP zaprojektowano w celu prostej implementacji funkcji protokołu HTTP i obsługi stron WWW w prostych konstrukcyjnie modułach i węzłach sieciowych. Wykorzystanie tych rozwiązań sieciowych pozwala na stosunkowo łatwą integrację różnych platform systemowych automatyki budynkowej BAS i przemysłowej oraz implementację nowych węzłów sieci. Możliwa jest również dzięki nim implementacja w strukturze sieciach automatyki budynkowej idei Smart Obiektów. Ze względu na fakt, iż wszystkie otwarte standardy dedykowane dla sieci BAS wykorzystują protokoły komunikacji bazujące na modelu ISO/OSI, wydaje się celowe odniesienie rozwiązań technologicznych i sieciowych proponowanych dla platformy IoT właśnie do struktury i kolejnych warstw tego modelu (patrz: Rys. 1). Przy czym należy zwrócić uwagę, że przy opracowywaniu protokołu IP do wykorzystania w sieciach IoT priorytetem jest redukcja długości słów danych przy zachowaniu ich kompatybilności z ogólnym standardem IP. Stąd pojawienie się w kolejnych warstwach protokołu nowych rozwiązań, zoptymalizowanych do obsługi zadań przypisanych do tychże warstw [12]



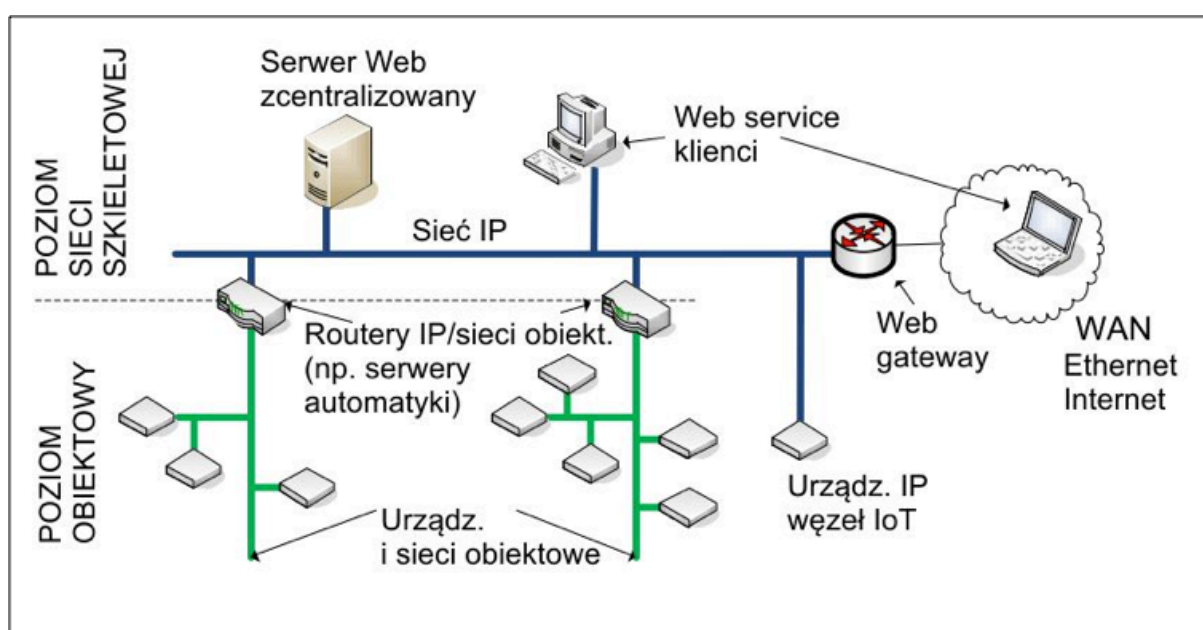
Rys. 1 – Protokoły sieci Internet i platformy IoT w odniesieniu do modelu ISO/OSI.

Jak już wspomniano wcześniej, integracja systemów BAS w ramach platform IoT musi uwzględniać zarówno włączenie do sieci Internetu Rzeczy istniejących już podsystemów magistralowych BAS różnych standardów, jak i nowych urządzeń, z wbudowanym już interfejsem IP.

W pierwszym z przypadków niezbędne jest zastosowanie modułów gateway, oferujących możliwość przekazu danych pomiędzy sieciami różnych standardów. W modułach tych preferuje się implementację różnych standardowych technologii (OPC, BACnet, LonWorks itd.), dzięki czemu moduł gateway'a może być „przezroczysty” dla sieci i przesyłanych przez nią komunikatów. Innym ważnym elementem integracji w platformie IoT sieci z magistralami obiektowymi otwartych standardów BAS jest decyzja dotycząca punktu/poziomu topologii sieci w którym integracja nastąpi. Możliwe są tu dwa scenariusze [11]:

- zcentralizowany – z dedykowanym serwerem usług Web, zapewniającym obsługę komunikacji danych i funkcjonalności dla grupy urządzeń systemów BAS powiązanych funkcjonalnie z takim serwerem, przez moduły gateway. Takie podejście jest prostsze w realizacji i nie wymaga angażowania dużych środków technicznych w istniejącej już strukturze sieci BAS oraz nadrzędnej sieci IP. Jednak cechuje się ograniczonymi możliwościami funkcjonalnymi i ogranicza niezależność węzłów sieci przyłączonych do magistral obiektowych. Nie jest możliwa bezpośrednia interakcja między węzłem sieci IP i pojedynczym węzłem sieci obiektowej, gdyż z punktu widzenia sieci IP interfejsem sieciowym węzła obiektowego jest obsługujący go serwer IP Web.
- zdecentralizowany – z implementacją usług i protokołu sieci IP bezpośrednio w węzłach sieciowych (czujniki, elementy wykonawcze, sterowniki itp.). Cechuje się wysokim poziomem autonomii węzłów sieci, jednak wymaga modernizacji lub wymiany modułów zainstalowanych wcześniej w ramach podsieci obiektowych.

Dlatego też, jak wskazują branżowi eksperci [13], w najbliższej przyszłości należy spodziewać się, iż implementacja rozwiązań komunikacyjnych IP w ramach platformy IoT w systemach automatyzacji budynków będzie hybrydą tych dwóch podejść integracyjnych. Przy czym tendencją będzie odejście od protokołów sieci obiektowych na korzyść rozwiązań bazujących na uniwersalnej sieci Internet, w szczególności w odniesieniu do nowych obiektów i budowanych w nich nowych sieci oraz przy modernizacji i rozbudowie już istniejących. Platformy takie, implementujące rozwiązania Internetu Rzeczy w budynkach zyskały w branży nazwę Building Internet of Things – BIoT [13][14]. Uproszczony schemat struktury i możliwej topologii sieci IoT (również BIoT), z elementami koncepcji zcentralizowanej i zdecentralizowanej pokazano na Rys. 2.



Rys. 2 – Struktura sieci IoT z elementami integracji zcentralizowanej i zdecentralizowanej.

We współczesnych aplikacjach systemowych automatyki budynkowej BAS wiele elementów infrastruktury widocznych na Rys. 2 już jest wykorzystywane. Sieci IP wykorzystywane są w nich jako platforma zdalnego dostępu do wybranych segmentów sieci, a za pośrednictwem tzw. serwerów automatyki do obsługi zmiennych sieciowych pojedynczych urządzeń obiektowych. Dzięki procedurom tzw. tunelowania komunikatów standardów sieci obiektowych, kanały IP poziomu nadrzędnego (szkieletowego), wykorzystuje się również do łączenia określonych linii sieci obiektowych lub większych podsieci. Nowością platformy IoT i BIoT będzie możliwość bezpośredniej wymiany danych między wszystkimi węzłami sieci, powiązanych funkcjonalnie, niezależnie od tego czy będą one fizycznie przyłączone do magistrali sieci obiektywnej, czy do kanału IP. Jak już wspomniano, docelowo wszystkie urządzenia sieciowe będą miały zaimplementowaną obsługę protokołu IP i działać będą jako

niezależne węzły sieciowe, współpracując w razie potrzeby z serwerami, routerami czy bazami danych, zależnie od przypisanych im zadań i funkcji w ramach platformy IoT.

Sieci domowe i budynkowe

Zaprezentowana forma rozwiązań technicznych i funkcjonalnych sieci sterowania oraz monitoringu w odniesieniu do budynków, rozwijana jest obecnie jako tzw. Smart Homes, czyli „inteligentne” domy i budynki. W obiektach takich implementowane są najnowsze technologie teleinformatyczne, multimedialne, systemy automatyki, zapewniające komfort i bezpieczeństwo samych budynków, jak i ich użytkowników oraz znajdującej się w nich infrastruktury. Możliwe jest to dzięki wymianie informacji na poziomie obiektowym pomiędzy czujnikami, sterownikami i elementami wykonawczymi, rozmieszczonymi w obiektach i odpowiedzialnymi za pracę różnych urządzeń i podsystemów. W branży pojawił się też termin Home Area Network – HAN (Sieci domowe), obejmujący platformy sieciowe, zwykle obiektowe i/lub niewielkie szkieletowe, integrujące wspomniane moduły systemowe, czujnikowe i wykonawcze. Wprowadzenie do tego typu struktur idei systemów Internetu Rzeczy IoT rozszerza ich możliwości oraz wprowadza nowe wymagania w odniesieniu do elementów systemowych. Wspomniane czujniki i elementy wykonawcze oraz moduły interfejsu do komunikacji z użytkownikami (komputery, panele dotykowe, smartfony itp.), włączane do sieci powinny się same skonfigurować, nawiązać połączenia z siecią i innymi jej węzłami, zapewniając możliwość zdalnego dostępu do nich, monitorowania i sterowania [3] [15]. Zadania i funkcjonalności dla urządzeń IoT Smart Home to między innymi:

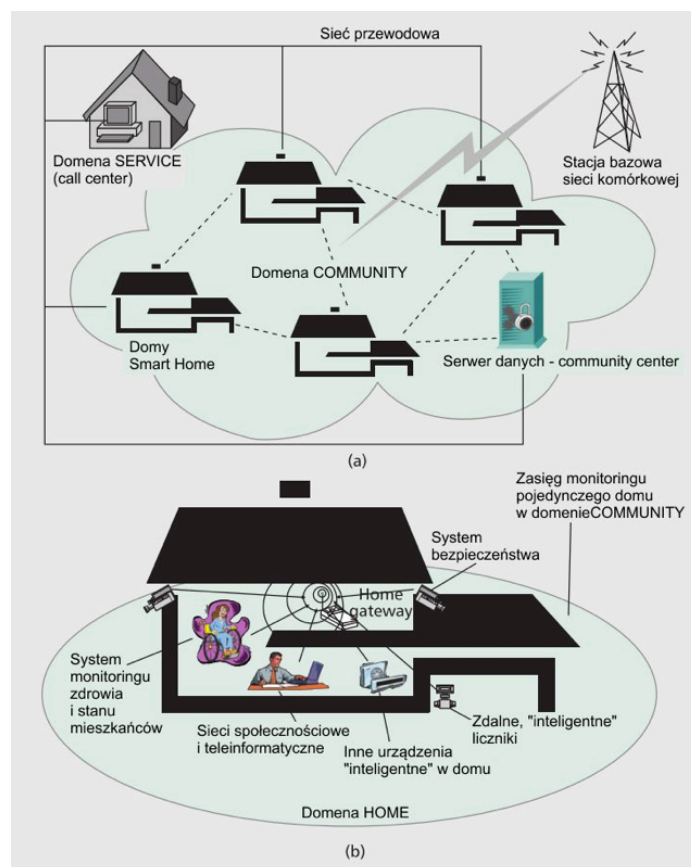
- wykrywanie zmian różnych parametrów fizycznych w domu, budynku
- szybkie reagowanie na zmiany, sygnały alarmowe
- rejestracja zachowań i przyzwyczajzeń użytkowników
- predykcja ich zachowań w najbliższej przyszłości
- interakcja z mobilnymi urządzeniami sterującymi i monitorującymi
- zapewnienie wygody użytkownika całego systemu i pewności działania poszczególnych jego funkcjonalności

Sieci typu Smart Home to rozwiązania dla pojedynczych domów, mieszkań. W odniesieniu do większych budynków lub zespołów budynkowych np. osiedle domków jednorodzinnych, jedną z propozycji wykorzystania najnowszych technologii komunikacji sieciowej jest organizacja tzw. Smart Społeczności (Smart Community – SC). Jest to idea lokalnych podsieci, powstających przy połączeniu sieciowym, bezprzewodowym lub przewodowym, kilku budynków, domów, które w sieci SC stają się węzłami z obsługiwanymi czujnikami i elementami wykonawczymi, monitorującymi parametry działania budynków, zachowania urządzeń i osób w budynkach.

Proponowana architektura systemu SC opiera się na trzech głównych elementach (patrz: Rys. 3) [15] [16]:

- Domena HOME – sieć automatyki i monitoringu w pojedynczym domu, budynku lub w wybranej strefie większego obiektu (np. piętro). Zapewnia monitoring parametrów urządzeń, środowiska w obiekcie, kontrolę obecności i zachowań osób itp. Komunikacja może być realizowana przez sieci z medium PowerLine, radiowe lub standardu IP (Ethernet). Dane przekazywane są do modułu home gateway, który posiada interfejsy sieciowych i konfigurację połączenia z innymi węzłami systemu SC.

- Domena COMMUNITY (Społeczność) – to kluczowy element systemu SC. Powstaje przez połączenie w sieci wymiany danych wszystkich modułów home gateway obiektów uczestniczących w Smart Społeczności. W ramach domeny COMMUNITY mogą być wymieniane dane pomiędzy uczestniczącymi w niej budynkami. W przypadku awarii połączenia sieciowego, przewidziano okresowe wsparcie komunikacji przez sieć telefonii komórkowej 3G. W domenie zlokalizowany jest ponadto indywidualny serwer danych (community center), gromadzący informacje od poszczególnych węzłów sieci (home gateway), z odpowiednimi zabezpieczeniami, autoryzacją dostępu itp.
- Domena SERVICE – centrum usług i obsługi uczestników domeny Społeczność. Jego kluczowym elementem jest łączność z jednostką np. straży miejskiej czy policji, która odbiera sygnały od mieszkańców (lub zgłaszane przez automatyczny system monitoringu) i na ich podstawie podejmuje działania zmierzające do jak najszybszej obsługi podmiotów, w celu zapewnienia im bezpieczeństwa i komfortu. Centrum może również, przy odpowiedniej organizacji i zezwoleniu ze strony mieszkańców, uczestniczyć w procesach rozliczeń np. dostaw energii i mediów itp.



Rys. 3 – Architektura systemu Smart Community: a) Domeny Community i Service; b) Domena Home.

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

Platforma IoT to idealne rozwiązanie technologiczne do obsługi transmisji danych pomiędzy wszystkimi elementami systemów Smart Społeczności, zarówno przy komunikacji między węzłami domen, jak i urządzeń wykonawczych i czujników, będących elementami ich infrastruktury, zainstalowanymi na poszczególnych budynkach.

Środowisko takie stwarza pole do realizacji różnego typu aplikacji. Badanymi obecnie [3][15] są:

- Zdalne opomiarowanie zużycia energii i mediów w budynkach. Dane z liczników zainstalowanych w poszczególnych budynkach (domeny HOME) przesyłane są do modułów home gateway, a z nich do zlokalizowanego w domenie Społeczność serwera community center. W serwerze dane są odpowiednio segregowane i przypisywane do kont poszczególnych uczestników domeny. Z serwera z kolei okresowo dane są wysyłane do centrum obsługi i stąd do odpowiednich podmiotów zewnętrznych w celach rozliczeniowych i/lub kontrolnych, ułatwiających zarządzanie popytem na energię i inne rodzaje mediów.
- Pomoc sąsiedzka – obserwacja otoczenia, szybkie reakcje na niepokojące zachowania osób, potencjalnie niebezpieczne sytuacje w otoczeniu domów itp. Domy wyposażone np. w kamery obserwujące otoczenie oraz czujniki wykrywające ruch w wybranych strefach otoczenia, po zarejestrowaniu sygnałów z tych obiektów, dzięki połączeniom sieciowym przekazują je do centrum serwisowego oraz/lub do innych uczestników domeny Społeczności. Dzięki temu możliwe jest szybkie reagowanie i podjęcie działań zapobiegawczych.

Zdarzeniami niebezpiecznymi mogą być również pożary, wykrywane przez odpowiednie czujniki, które przekazują informacje do systemu monitorującego, z możliwością bezpośredniego przekierowania do central odpowiednich służb (straż pożarna, policja).

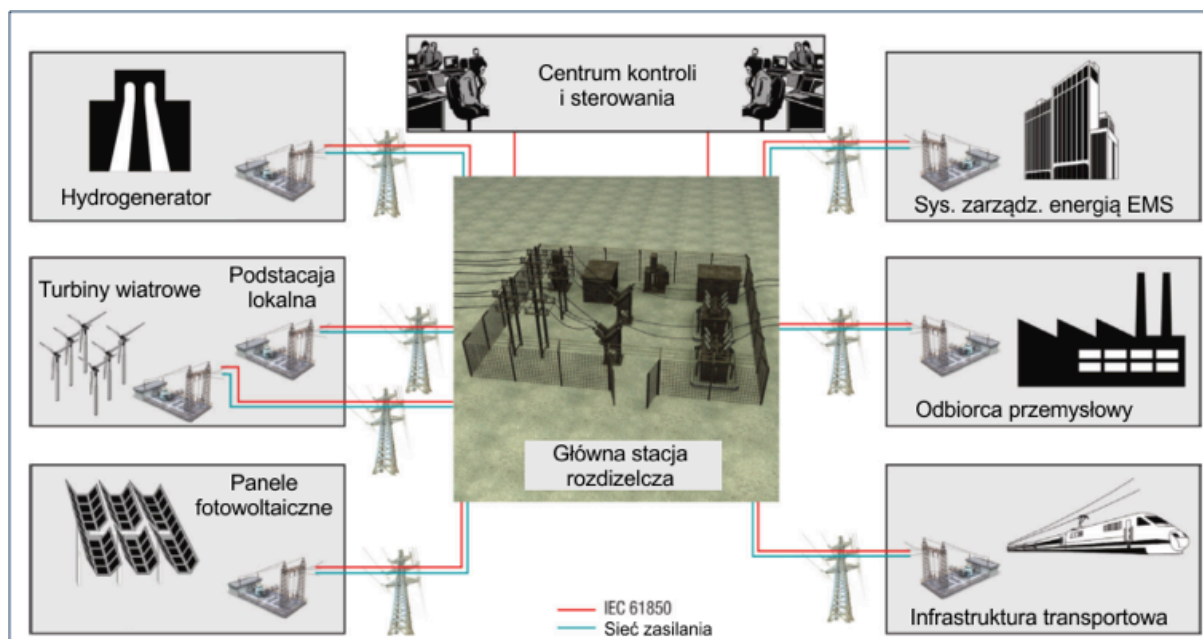
- Telemedycyna – zdalny monitoring stanu zdrowia osób starszych lub z przewlekłymi chorobami, zagrażającymi życiu lub bezpieczeństwu osób. Obsługa strumieni danych z czujników/modułów bezprzewodowych, zlokalizowanych w ubraniach chorych lub na ich ciele.
- Wykorzystanie sieci lokalnych w ramach domen Społeczności, jako środowiska do wzajemnych kontaktów i wymiany informacji pomiędzy mieszkańcami.

Wszystkie przedstawione koncepcje wykorzystania technologii Internetu Rzeczy w budynkach, wymagają jednak kompleksowego podejścia do organizacji jego infrastruktury, zarówno stricte budowlanej, jak i instalacyjnej, sieciowej i poszczególnych podsystemów [12] [16]. Dlatego też w niniejszym opracowaniu przedstawiona zostanie koncepcja wytycznych dla organizacji systemów IoT w budynkach, zarówno na poziomie obiektowym, jak i nadrzędnym, z ukierunkowaniem na zapewnienie integralności sterowników, czujników i elementów wykonawczych oraz ich zdalnej obsługi i wykorzystania w sieciach systemowych zarządzania i sterowania budynkami – BMS.

5. Sieci IoT w energetyce – Smart Grid

Ciągły wzrost zapotrzebowania na energię elektryczną oraz coraz częstsze instalacje różnego typu źródeł odnawialnych, przyłączanych do systemu elektroenergetycznego, to główne czynniki determinujące konieczność zmian koncepcji jego organizacji i funkcjonowania w nowych realiach rynkowych i technicznych. Stąd idea implementacji rozwiązań komunikacji sieciowej między różnymi elementami systemu elektroenergetycznego, która ułatwi zarządzanie rozpiętką mocy w systemie, pozwoli na wprowadzenie do niego pewnej dynamiki zarządzania mocą w zależności od zmieniającego się zapotrzebowania na energię oraz dostaw lokalnych, ze źródeł odnawialnych. Koncepcja ta nosi nazwę inteligentnych sieci – Smart Grid. To termin używany obecnie przez wszystkie podmioty zaangażowane w branżę energetyczną, a najczęściej kojarzony głównie z koniecznością implementacji tzw. inteligentnych liczników energii (zdalnego odczytu) oraz modułów monitorujących pracę podstacji rozdzielczych. Dopiero w dalszej perspektywie jawi się funkcjonalność zdalnego zarządzania popytem na energię w sieci dystrybucyjnej oraz sprawna obsługa rozproszonych źródeł i zasobników energii (prosumenci) [17]. Wzrost popularności tych ostatnich powoduje konieczność nowego podejścia do organizacji systemu elektroenergetycznego, zwłaszcza na poziomie lokalnym. Stąd koncepcja organizacji tzw. mikroinstalacji, obejmujących pojedyncze budynki lub zespoły budynków i związaną z nimi infrastrukturę, wraz z przyłączonymi odnawialnymi źródłami energii. Wyraźna tendencja do rozproszenia generacji energii w systemie gdzie oprócz dominujących producentów, dużych elektrowni, pojawiają się źródła lokalne o większej lub mniejszej mocy oraz zmiennej wydajności (uzależnionej w dłuższych okresach czasu np. od warunków pogodowych – wiatr, nasłonecznienie), wymaga sprawnej obsługi i efektywnego zarządzania energią i mocą dostępną w systemie elektroenergetycznym. W najbliższej perspektywie rozwojowej prowadzi to do konieczności implementacji rozproszonych modułów monitorujących i sterujących, wyposażonych w mikroprocesory o stosunkowo niewielkich mocach obliczeniowych i interfejsy komunikacji sieciowej. Ich rozmieszczenie w rozdzielniach, podstacjach itp. umożliwi dokładniejsze monitorowanie rozpiętków mocy w systemie, prowadzenie pomiarów zużycia energii oraz wykrywanie strat w określonych obszarach zasilania, a w konsekwencji lepsze sterowanie i adaptację systemu do zmieniających się uwarunkowań systemowych [3][6][18].

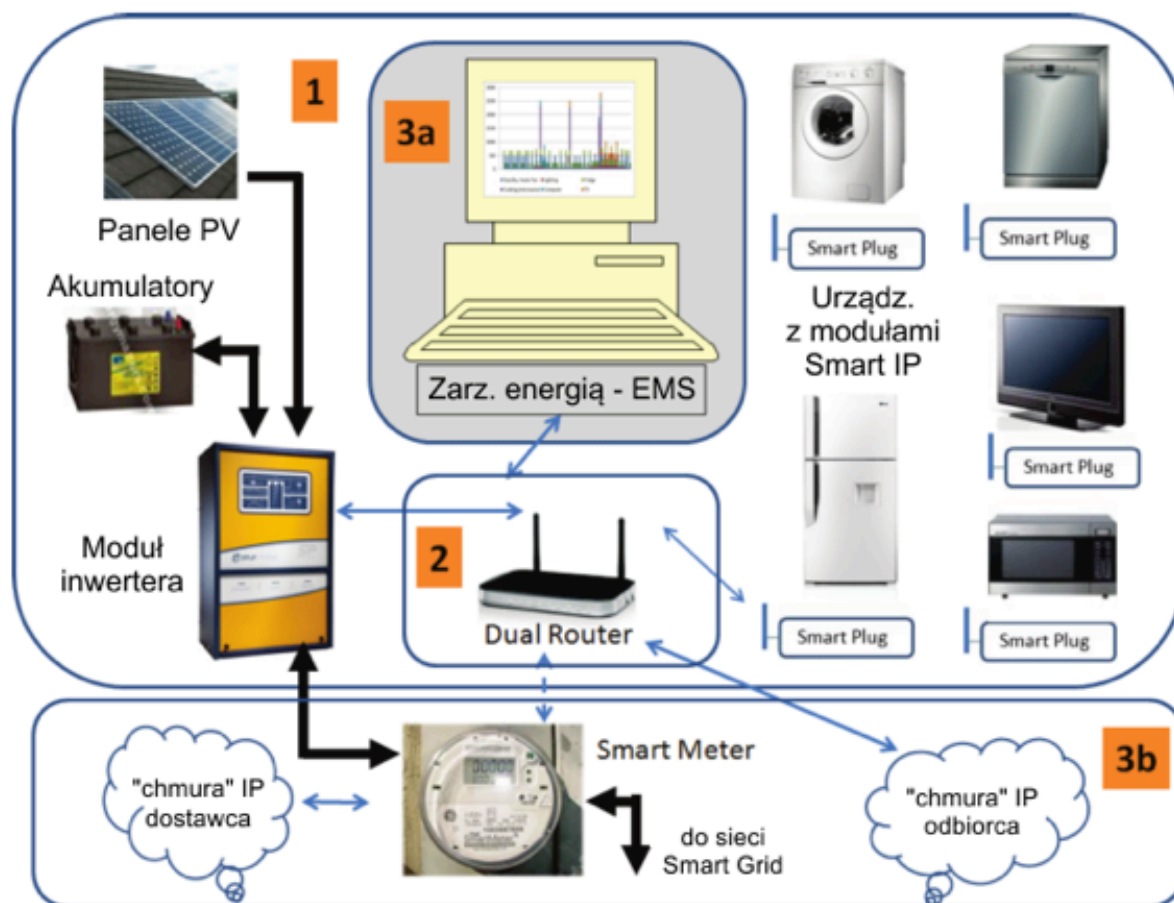
Internet Rzeczy jako platforma komunikacyjna wspierająca realizację idei Smart Grid może być wykorzystana w różnych aspektach. Jednym z nich jest wspomniana już perspektywa rozproszenia generacji oraz wdrożenia „aktywnych” systemów zarządzania popytem Demand-Response, wraz z narzędziami dokładniejszego, bardziej efektywnego zarządzania energią i mocą w systemie dystrybucyjnym. Wymagać ona będzie poszerzenia funkcjonalności i obszarów zastosowania sieciowej komunikacji danych u samych odbiorców, dystrybutorów, dostawców oraz pomiędzy tymi podmiotami. Ważnym elementem struktury systemu dystrybucji energii są podstacje, w których dokonuje się transformacja napięcia w sieci, rozdział mocy, zarządzanie i koordynacja mocy pozyskiwanych z lokalnych źródeł odnawialnych oraz likwidacja ewentualnych awarii, przerw w dostawach prądu itp. [19]. Schemat struktury takiej podstacji z elementami obsługiwaną infrastrukturą, pokazano na Rys. 4.



Rys. 4 – Sieć zasilania i komunikacji – stacja rozdzielcza i podstacje lokalne.

W nowej koncepcji inteligentnego systemu elektroenergetycznego odgrywać one będą niebagatelną rolę. W ich obsłudze otwiera się szerokie pole do zastosowania technologii Internetu Rzeczy IoT. Możliwość sprawnego, prowadzonego również w czasie rzeczywistym lokalizowania, mapowania monitorowania i sterowania podstacji na poziomie dzielnicy, miasta, województwa i całego kraju, to elementy, dzięki którym rozproszona sieć komunikacji zapewni lepsze funkcjonowanie systemu elektroenergetycznego. Dlatego w oparciu o standard IEC 61850 z protokołem IP, w podstacjach instalowane są moduły monitorująco-sterujące i koncentratory sygnałów, które zapewniają obsługę zaawansowanej infrastruktury pomiarowej (AMI), danych z różnego rodzaju czujników rozlokowanych w podstacjach oraz mierników energii – głównych w podstacji oraz tzw. sub-liczników zlokalizowanych w podsieciach lokalnych lub bezpośrednio u odbiorców. Dane z wszystkich tych urządzeń mogą być przekazane do nadrzędnych aplikacji zarządzania lub transmitowane bezpośrednio między modułami, w celu lokalnego prowadzenia procedur regulacji, sterowania mocą, operacji zarządzania popytem itp. [19].

Na najniższym poziomie sieci komunikacyjnych i transmisji danych w systemach Smart Grid zlokalizowani są odbiorcy. Wdrożenie rozwiązań sieciowych Internetu Rzeczy nabiera szczególnie istotnego znaczenia w ich obsłudze, zwłaszcza zaś tych odbiorców którzy posiadają lub będą posiadać w infrastrukturze systemu zasilania źródła odnawialne (wspomniani już wcześniej prosumenci). W budynkach i obiektach użyteczności publicznej lub zakładach przemysłowych coraz więcej urządzeń powszechnego użytku, przyłączanych do sieci zasilania, jest jednocześnie wyposażonych w moduł komunikacji internetowej – patrz: rysunek 5 [17][18][20].



Rys. 5 – Architektura systemu prosumenta: 1-urządzenia i czujniki; 2-moduł Gateway IP; 3-aplikacje obsługi odbiorcy-prosumenta.

Po zaimplementowaniu odpowiednich aplikacji i algorytmów działania, mogą one komunikować się między sobą, ale również reagować na sygnały i dane informacyjne przesyłane przez dystrybutorów energii, chociażby w celu załączenia lub wyłączenia urządzeń w określonych okresach czasu, w różnych taryfach rozliczeniowych energii, zależenie od aktualnego poziomu obciążenia linii zasilającej czy np. wprowadzonej do systemu sterowania i zarządzania budynkiem BMS informacji o nieobecności użytkowników lub okresie wakacyjnym [3][18]. Wykorzystanie protokołu IP zagwarantuje w razie potrzeby, zdalny dostęp do tych urządzeń i modułów, oczywiście przy uwzględnieniu odpowiednich priorytetów i weryfikacji uprawnień klienta. Standard sieci Internetowej pozwoli na wykorzystanie w tym celu popularnych i ogólnie znanych narzędzi dostępowych, takich jak przeglądarka internetowa czy aplikacje smartfonów, tabletów itp. Na poziomie odbiorcy ważnym elementem są i będą liczniki zdalnego odczytu (idea inteligentnego opomiarowania Smart Metering). Liczniki, przekazujące dane dotyczące zużycia energii i mediów, nie tylko do nadrzędnych modułów sterujących, akwizycji danych

czy rozliczeń, ale również bezpośrednio do innych urządzeń przyłączonych w sieci domowej czy domenie Społeczność, dzięki integracji w sieci IoT, pozwolą na organizację bardziej efektywnych systemów zarządzania energią – EMS. Ważnym elementem tej organizacji są właściwe wytyczne w zakresie wzajemnych powiązań funkcjonalnych różnych urządzeń: czujników, liczników i elementów wykonawczych, zintegrowanych w strukturze systemu EMS, wraz z algorytmami sterowania. Możliwe jest tu wykorzystanie na poziomie obiektowym również sieci automatyki budynkowej, elementów systemowych BMS oraz ustandaryzowanych profili funkcjonalnych dla węzłów sieciowych takich systemów. Warto podkreślić, że i w tym obszarze koncepcja IoT zdobywa coraz większą popularność i jest oferowana przez uznanych producentów urządzeń automatyki budynkowej[3][6].

6. Internet Rzeczy w wybranych aplikacjach

Jak już wspomniano na samym początku raportu, Internet Rzeczy to rozwiązanie technologiczne zapewniające komunikację i wymianę danych pomiędzy ludźmi (komputery, tablety, smartfony, panele mobilne), ale również między ludźmi a urządzeniami oraz bezpośrednio pomiędzy różnymi urządzeniami, modułami sterowania, monitoringu i wykonawczymi, bez udziału człowieka – IIoT (Industrial Internet of Things) i M2M. Trzeba podkreślić, że wiele urządzeń już działa w ramach tej koncepcji. Jak wskazują dostępne raporty i analizy na początku 2010 roku Internet Rzeczy tworzyło prawie 12,5 mld urządzeń, a według szacunków w 2015 roku liczba ta ma wynosić 25 mld urządzeń, zaś w kolejnej perspektywie roku 2020 już nawet 50 mld [21]. Tak burzliwy i dynamiczny rozwój stymulują obserwowane już obecnie wytężone prace wielu inżynierów i naukowców, wielu komercyjnych firm i ośrodków badawczych, nad szeroko pojętą grupą urządzeń i usług realizujących ideę Internetu Rzeczy. Przykładowo Daimler Group inwestuje w rozwój usług mobilnych typu car2go, myTaxi czy moovel, zorientowanych na usprawnienie komunikacji w ośrodkach miejskich. General Electric do obsługi urządzeń i fabryk używa systemu pod nazwą „Industrial Internet” (Internet przemysłowy); LG przygotowuje ofertę pod „inteligentne domy”, produkując już telewizory i urządzenia AGD, które mogą łączyć się z Internetem, wzbogacając ofertę o powiązane z nimi usługi, również te związane z wspomnianymi wcześniej systemami zarządzania budynkiem BMS czy energią EMS [22]. Urządzenia AGD (inteligentne lodówki, pralki, termostaty) obsługiwane zdalnie przez mobilną aplikację, drzwi otwierane smartfonem, czy też ubrania dla dzieci z czujnikami, które powiadomią rodziców, gdy maluch jest głodny, to kolejne przykłady urządzeń komunikujących się wzajemnie w ramach IoT, które już istnieją i są prezentowane podczas wystaw i targów, np. CES 2014 (Consumer Electronics Show). Dzięki nim wzrasta komfort życia, bezpieczeństwo oraz efektywność energetyczna. Dobrym przykładem w tym zakresie może być nowoczesna, interaktywna lodówka, która sama dokona analizy przechowywanych w niej produktów (np. ich ilość, termin przydatności do spożycia, propozycja posiłku), podejmie decyzje, a następnie skontaktuje się ze sklepem (w którym zamówienia będą przyjmowały i realizowały maszyny), zapłaci i być może odbierze nawet zamówienie, gdy przywiezie je autonomiczny samochód. Na koniec wystawi ocenę innym maszynom uczestniczącym w tym procesie. Przegląd urządzeń elektroniki użytkowej, sterowania i monitoringu, pozwala na wyróżnienie kilku grup modułów dedykowanych do współpracy w ramach IoT:

- bezpośrednio związane z użytkownikiem
- interaktywne czujniki wszyte w ubrania

- nowoczesne zegarki, breloki lub opaski mierzące różne parametry, z akwizycją danych
- „inteligentne” okulary bezprzewodowo komunikujące się z Internetem
 - związane z domem/budynkiem
- czujniki monitorujące parametry w budynku
- nowoczesne zdalnie sterowane źródła światła
- efektywne sterowanie ogrzewaniem
- zdalnie sterowane gniazdka elektryczne - proste sterowanie urządzeń
- bezprzewodowa obsługa zamków w drzwiach – kontrola dostępu
- domowi asystenci medyczni - inteligentne sieci zdrowia, telemedycyna
- bezprzewodowa obsługa roślin domowych
 - związane z otoczeniem (np. infrastruktura miasta)
- oświetlenie przestrzeni publicznych
- systemy informacji i nawigacji
- usprawnienie procesów utrzymania mienia
- informacje o wydarzeniach i zagrożeniach
- zdalny monitoring i reagowanie na zdarzenia
 - związane z przemysłem
- optymalizacja procesów produkcji oraz transportu i logistyki
- poprawa bezpieczeństwa
- poprawa efektywności procesów i obsługi maszyn
 - związane ze środowiskiem
- monitorowanie poziomu zanieczyszczeń powietrza i wody
- ochrona zasobów przyrody i dzikich zwierząt
- zdalny monitoring parametrów pogodowych - reagowanie i ostrzeżenie

Technologia IoT w zarządzaniu infrastrukturą budynków

W okresie ostatnich dwóch lat zaobserwować można wyraźną tendencję przystosowywania urządzeń automatyki przemysłowej i budynkowej oraz elementów systemów zarządzania budynkami BMS, do pracy w ramach technologii Internetu Rzeczy. W przypadku infrastruktury budynków będącej w praktyce zbiorem różnych urządzeń i podsystemów, można wskazać wiele przykładów modułów dostępnych już na rynku, wyposażonych w interfejs protokołu IP i otwartych na implementację w ramach sieci Internet. W tabeli 1 wyróżniono najważniejsze podsystemy spotykane w nowoczesnych obiektach budowlanych, wraz z przykładowymi urządzeniami oraz elementami IoT proponowanymi jako wsparcie ich obsługi.

Lp	Podsystem	Przykład urządzeń	Elementy platformy systemowej IoT
1	Sterowanie HVAC	sterowniki, termostaty	Interfejs IP (przewodowy lub bezprzewodowy), zdalna obsługa i monitoring
2	Sterowanie oświetleniem Sterowanie roletami, żaluzjami, markizami	oprawy, sterowniki	Moduły wyposażone w układy MCU zapewniające sterowanie elementami wykonawczymi oraz komunikację bezprzewodową
3	Systemy sygnalizacji włamania i napadu (SSWiN), Systemy kontroli dostępu (SKD)	czujniki obecności, moduły komunikacyjne wideo-domofony	Interfejs IP (przewodowy lub bezprzewodowy), zdalna obsługa i monitoring (enkrypcja SSL/TLS i AES-256bit), integracja z sieciami telekomunikacyjnymi; Skalowalność
4	Systemy telewizji dozorowej (CCTV)	kamery, rejestratory	Interfejs IP (możliwość PoE), Implementacja usług: VLAN, QoS, redundancja sieci; Mobilność - użytkownicy urządzeń mobilnych mogą przeglądać nagrania monitoringu w czasie rzeczywistym; Nadzór wideo w chmurze; Otwarte protokoły sieciowe - ułatwienie integracji; Skalowalność, Zdalny dostęp, Poprawa jakości audio/video wraz ze wzrostem przepustowości sieci; Wykorzystanie okablowania strukturalnego - łatwość montażu
5	Monitoring zużycia energii elektrycznej i ciepłej	liczniki, analizatory, koncentratory danych	Interfejs IP, możliwość akwizycji i przetwarzania danych w dowolnym miejscu na świecie, zdalne załączanie i wyłączanie odbiorów; sieci domowe; dwukierunkowa komunikacja z operatorami systemów dystrybucji i sprzedaży energii, mediów
6	Instalacje A/V (Audio/Video)	Telewizory, kino domowe,	Interfejs IP, system operacyjny umożliwiający obsługę urządzeń w budynku
7	Sterowanie urządzeniami RTV/AGD	sterowane gniazdka	Komunikacja za pomocą sieci bezprzewodowych lub sieci elektroenergetycznych; złączanie i wyłączanie dowolnego urządzenia za pomocą urządzeń mobilnych - z dowolnego miejsca, Informacja w czasie rzeczywistym o stanie pracy
8	Sterowanie oświetleniem przestrzeni wokół budynku	routery, sterowniki pracujące w ramach sieci kratowych	Zdalna obsługa i monitoring; komunikacja z służbami serwisowymi i obsługi
9	Czujniki, sensory	temperatura, ciśnienie, natężenie oświetlenia, CO ₂ , wilgotność	zastosowanie IP poprzez zaimplementowanie technologii 6LoWPAN, bezprzewodowa komunikacja dwukierunkowa, zasilanie za pomocą technologii <u>energy harvesting</u> , komunikacja bezprzewodowa jako ułatwienie montażu, szczególnie w trudnodostępnych miejscach
10	Moduły wejść/wyjść	moduł wejść/wyjść cyfrowych lub analogowych	Interfejs IP, zdalna obsługa i monitoring

Tabela 1 – Kategorie podsystemów infrastruktury budynków wraz z elementami platformy IoT.

Lp

Podsystem

Przykład urządzeń

Elementy platformy systemowej IoT

1

Sterowanie HVAC

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

sterowniki,
termostaty

Interfejs IP (przewodowy lub bezprzewodowy), zdalna obsługa i monitoring

2

Sterowanie oświetleniem

Sterowanie roletami, żaluzjami, markizami

oprawy,

sterowniki

Moduły wyposażone w układy MCU zapewniające sterowanie elementami wykonawczymi oraz komunikację bezprzewodową

3

Systemy sygnalizacji włamania i napadu (SSWiN), Systemy kontroli dostępu (SKD)

czujniki obecności,

moduły komunikacyjne

wideo-domofony

Interfejs IP (przewodowy lub bezprzewodowy), zdalna obsługa i monitoring (enkrypcja SSL/TLS i AES-256bit), integracja z sieciami telekomunikacyjnymi; Skalowalność

4

Systemy telewizji dozorowej (CCTV)

kamery,

rejestratory

Interfejs IP (możliwość PoE), Implementacja usług: VLAN, QoS, redundancja sieci;

Mobilność - użytkownicy urządzeń mobilnych mogą przeglądać nagrania monitoringu w czasie rzeczywistym; Nadzór wideo w chmurze; Otwarte protokoły sieciowe - ułatwienie integracji; Skalowalność, Zdalny dostęp, Poprawa jakości audio/video wraz ze wzrostem przepustowości sieci; Wykorzystanie okablowania strukturalnego - łatwość montażu

5

Monitoring zużycia energii elektrycznej i ciepłej

liczniki,

analizatory,

koncentratory danych

Interfejs IP, możliwość akwizycji i przetwarzania danych w dowolnym miejscu na świecie, zdalne załączanie i wyłączanie odbiorów; sieci domowe; dwukierunkowa komunikacja z operatorami systemów dystrybucji i sprzedaży energii, mediów

6

Instalacje A/V (Audio/Video)

Telewizory, kino domowe,

Interfejs IP, system operacyjny umożliwiający obsługę urządzeń w budynku

7

Sterowanie urządzeniami RTV/AGD

sterowane gniazdko

Komunikacja za pomocą sieci bezprzewodowych lub sieci elektroenergetycznych; złączanie i wyłączanie dowolnego urządzenia za pomocą urządzeń mobilnych - z dowolnego miejsca, Informacja w czasie rzeczywistym o stanie pracy

8

Sterowanie oświetleniem przestrzeni wokół budynku

routery,

sterowniki pracujące w ramach sieci kratowych

Zdalna obsługa i monitoring; komunikacja z służbami serwisowymi i obsługi

9

Czujniki, sensory

temperatura,

ciśnienie,

natężenie oświetlenia,

CO₂,

wilgotność

zastosowanie IP poprzez zaimplementowanie technologii 6LoWPAN, bezprzewodowa

komunikacja dwukierunkowa, zasilanie za pomocą technologii energy harvesting,

komunikacja bezprzewodowa jako ułatwienie montażu, szczególnie w trudnodostępnych miejscach

10

Moduły wejść/wyjść

moduł wejść/wyjść cyfrowych lub analogowych

Interfejs IP, zdalna obsługa i monitoring

Technologie będące podstawą systemową Internetu Rzeczy oferują nowe możliwości zdalnego sterowania urządzeń gospodarstwa domowego, wyposażenia i podsystemów infrastruktury budynków, a ich interfejsy komunikacyjne nowej generacji pozwalają na transformację modułów i urządzeń występujących w otoczeniu człowieka z pasywnych na w pełni interaktywne, „inteligentne”, tworzące aktywne środowisko usług, z zapewnieniem ciągłego dostępu do różnorodnych usług i zasobów. Jednakże przegląd dostępnych, rozwijanych obecnie i wprowadzanych na rynek urządzeń (systemów sterowania, elektroniki konsumenckiej, AGD) wskazuje, że tylko niewielki ich odsetek jest gotowy do pracy w ramach w pełni zintegrowanej platformy systemowej systemu IoT, jako podstawy zintegrowanego systemu sterowania i zarządzania budynkiem. Koncepcje, zalety oraz problemy dotyczące takiej integracji systemów zarządzania i sterowania zostały już w dużym stopniu zidentyfikowane i określone w ramach wielu prac badawczo-rozwojowych technologii dla systemów automatyki przemysłowej i automatyki budynkowej [2][10][23]. Naturalnym niemal krokiem wydaje się zatem użycie wypracowanych narzędzi i mechanizmów różnych urządzeń IoT, przeznaczonych do pracy w różnych aplikacjach budynkowych, w ramach systemów automatyki budynkowej (BAS). Niestety wnioski z analizy funkcjonalnej oraz możliwości komunikacji danych dla urządzeń dostępnych na rynku (w ramach przytoczonych wcześniej przykładów, wskazują, że są to najczęściej produkty firmowe, realizujące określone funkcjonalności. Często w nowoczesny, innowacyjny sposób (zdalne sterowanie za pomocą smartfonu, monitoring mobilny itp.), jednak bez uwzględnienia potrzeby pełnej integracji urządzeń sterujących i wykonawczych, w szczególności z innymi podsystemów infrastruktury budynkowej. Przypomina to sytuację z przed kilkunastu lat z branży systemów automatyki przemysłowej i budynkowej, gdzie dominowały rozwiązania firmowe, ograniczające możliwości funkcjonalne użytkowników i wiążące ich z ofertą tylko jednej firmy.

Tymczasem obecnie w branży sieci automatyki podstawą oferty są standardy otwarte, pozwalające na swobodne łączenie fizyczne i funkcjonalne modułów pochodzących od różnych producentów, komunikujących się pomiędzy sobą za pośrednictwem ustandaryzowanych platform systemowych. Takie rozwiązania coraz częściej są stosowane

przede wszystkim w dużych budynkach użyteczności publicznej, kompleksach budynkowych, biurach i obiektach komercyjnych. W ramach jednolitego systemu komunikacji sieciowej integruje się wszystkie podsystemy infrastruktury budynków, co daje możliwość budowania złożonych funkcjonalności, wspierających efektywne zarządzanie, monitoring i sterowanie.

Jednakże znaczenie pełnej i bezproblemowej integracji systemów automatyki jest istotne nie tylko na terenie dużego budynku, zespołu budynków czy wręcz w skali miasta, ale również coraz częściej w niewielkich budynkach mieszkalnych, wielorodzinnych i domach jednorodzinnych, które powoli stają się istotnym i pełnoprawnym elementem np. inteligentnych sieci energetycznych (Smart Grid). Zintegrowane systemy zarządzania i monitoringu BMS mogą być bardzo przydatne we wsparciu realizacji wspomnianej już wcześniej idei prosumentów, szczególnie w perspektywie instalacji lokalnych źródeł odnawialnych oraz wprowadzenia inteligentnych liczników energii (monitoring, zarządzanie popytem na energię) [17][24].

W sukurs przychodzą jednak podejmowane coraz szerzej działania, zmierzające do implementacji na różnych poziomach aplikacyjnych w sieciowych systemach automatyki budynkowej, elementów technologii Internetu Rzeczy i urządzeń AGD oraz wyposażenia budynków, konstruowanych zgodnie ze wspomnianą już wcześniej ideą Smart Obiektów. Oparte o protokół IPv6 interfejsy nowej generacji powodują postępującą migrację modułów i urządzeń z otoczenia człowieka, z pasywnych w kierunku silnie interaktywnych, „inteligentnych”, tworzących aktywne środowisko usług z dostępem do różnorodnych zasobów.

Rozpowszechniający się dostęp do szerokopasmowych sieci teleinformatycznych, wraz z rozwojem zaawansowanych usług sieciowych, oferuje możliwość ich wykorzystania w bezpośrednim, codziennym otoczeniu człowieka.

Na rynku obserwowalny jest również ciągły rozwój oferty nowoczesnych, zaawansowanych funkcjonalnie komponentów systemowych (czujniki, moduły komunikacji przewodowej i bezprzewodowej, wydajnych jednostek obliczeniowych, etc.), służących do budowy lub projektowania platform urządzeń automatyki nowej generacji, zgodnych z ideą IoT.

Przykładami grup tego typu elementów są:

- interfejsy komunikacyjne przewodowe i bezprzewodowe - protokołów, które mogą zostać wykorzystane podczas realizacji platformy systemowej IoT
 - Ethernet - np. Marvell,
 - PLC - np. Echelon,
 - GNSS, GPS, GLONASS, Galileo, QZSS, BeiDou, SBAS - np. CSR,
 - WiFi - np. apm communication, CSR, Microchip,
 - RF - np. Semtech, Silicon Labs,
 - ZigBee - np. Microchip, Telegesis, Silicon Labs,
 - Bluetooth - np. Microchip, CSR, Lair,
 - GSM - np. Sierra Wireless, Quectel,
- czujniki - np. Microchip, Semtech, Silicon Labs, Cirrus Logic, Maxim integrated
 - parametrów środowiskowych - temperatura, ciśnienie, natężenie oświetlenia, etc.,
 - analogowe - 0-5V, 0-10V, 0-20 mA, termistorowe, styk bezpotencjałowy, otwarty kolektor,
 - parametrów energetycznych,
- mikrokontrolery MCU - np. Silicon Labs, Microchip, Renesas
 - mikrokontrolery ARM,
 - mikrokontrolery o ultraniskim poborze mocy,

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

- mikrokontrolery z wbudowanym modułem komunikacji bezprzewodowej,
- moduły zarządzania energią - np. Intersil, Maxim, Microsemi, Semtech, Silicon Labs
- układy ładowania i zabezpieczania wykorzystujące zjawisko energy harvesting,
- układy ładowania Li-Ion,
- zabezpieczenia obwodów,
- sterowniki PoE,
- regulatory ładowania,
- platformy rozwojowe
- Arduino,
- Raspberry Pi,
- BeagleBone Black,
- OpenPicus,
- Libelium Wasmote,
- narzędzia programistyczne
- Wylless,
- Node-RED,
- WebIOPi

Wszystkie te elementy i platformy technologiczne otwierają nowe możliwości w zakresie konstrukcji różnego typu modułów, również tych dedykowanych obsłudze funkcjonalności związanych z automatyzacją budynków.

Platforma rozwojowa IoT dla automatyki budynkowej (IzoT)

Jedną z ciekawszych propozycji platform rozwojowych urządzeń automatyki budynkowej w kierunku ich wykorzystania i integracji w ramach platformy sieciowej IoT, jest oferta firmy Echelon. Warto przypomnieć, iż jest to firma od wielu lat zaangażowana w rozwój jednego z międzynarodowych, otwartych standardów sieci automatyki budynkowej PN-EN ISO/IEC 14908 (LonWorks). Sieci sterowania i monitoringu budynków bazujące na tym standardzie funkcjonują w wielu budynkach na świecie, w licznych aplikacjach przemysłowych i komercyjnych.

Zaproponowana nowa platforma IzoT składa się z układów MCU (FT 6050, Neuron 6000), modułów komunikacyjnych (Wi-Fi, RF 802.15.4 i innych) oraz stosów 16, 32 i 64 bitowego (IzoT Device Stack EX, IzoT Device Stack DX, IzoT Server Stack). Obejmuje ona także routery IzoT - będące interfejsem pomiędzy różnymi typami nośników i kanałów (różne media transmisyjne) oraz niezbędne narzędzia do obsługi usług sieciowych i integracji sieci. IzoT to również rodzina protokołów aplikacji i łącza, bazująca na IPv6 i IPv4. Protokoły aplikacji IzoT to m.in. IzoT/IP oraz BACnet/IP. W urządzeniach IzoT możliwe jest zaimplementowanie także innych protokołów aplikacji, które korzystają z warstwy transportowej IP IzoT: na przykład, urządzenia IzoT mogą wykorzystywać protokół Modbus TCP lub inne dedykowane protokoły sieci sterowania przemysłowych i budynkowych. Protokół IzoT/IP bazuje na usługach zawartych w warstwie siódmej protokołu LonTalk, zapewnia zgodność z warstwami 3 do 6 standardu ISO/IEC 14908-1, wraz z natywnym adresowaniem IP w warstwie 3 oraz z protokołami łącza, specyficznymi dla warstw 1 i 2. Możliwe jest realizowanie kompresji pakietów warstwy 3 w zależności od wymagań protokołów komunikacyjnych. IzoT/IP może

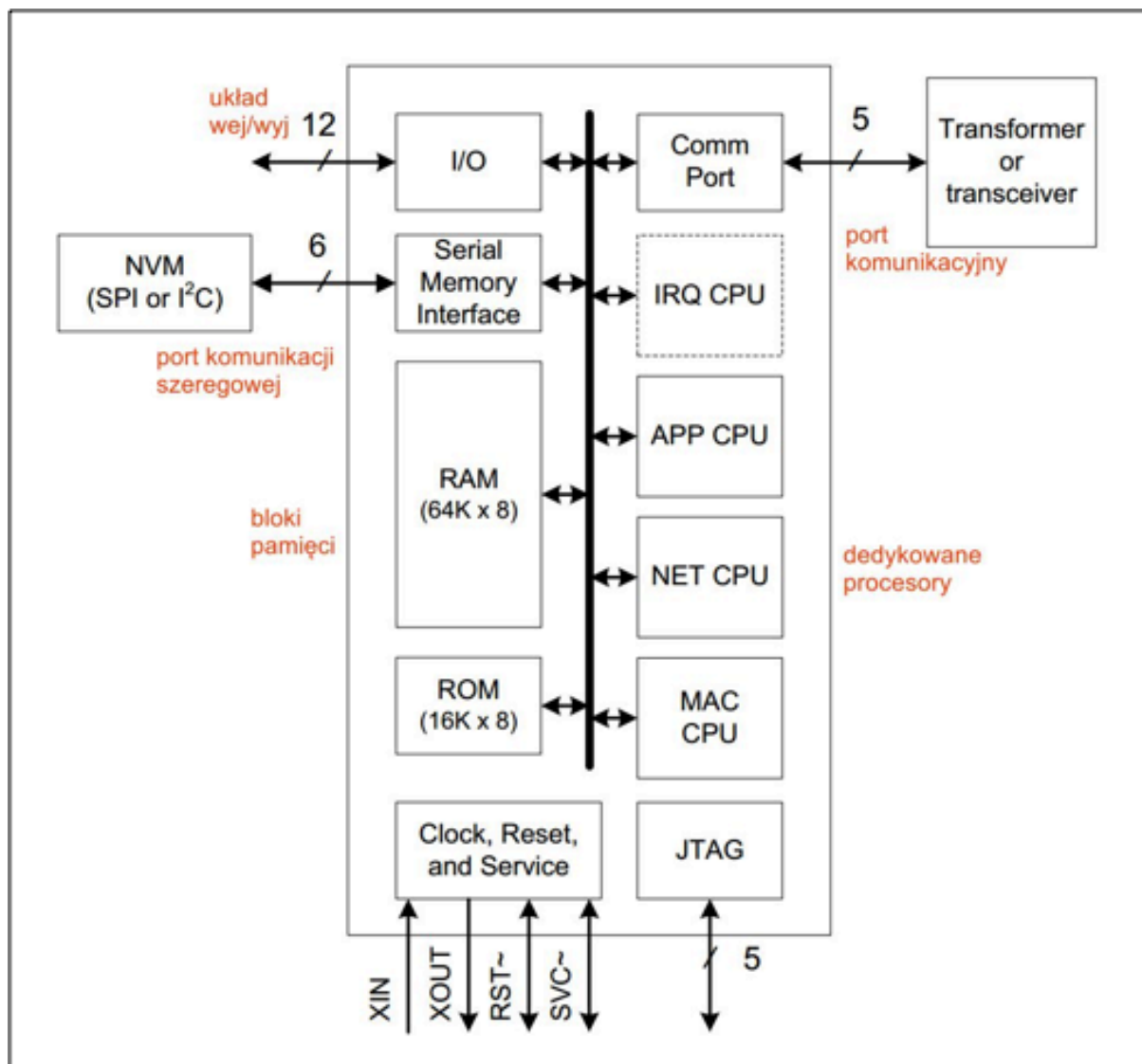
Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

być stosowany wraz z dowolnym łączem kompatybilnym z protokołem IP. Łączy powszechnie stosowane to: Ethernet /IP (IzoT /EN), Wi-Fi (IzoT/ Wi-Fi), RF 802.15.4 (IzoT / RF), oraz ISO/IEC 14908-2, zgodne z topologią pary skręconej (IzoT/FT) [25].

IzoT Router – wielokanałowy router i lokalny serwer platformy IzoT. Zapewnia urządzeniom IzoT i LonWorks, podłączonym do różnych rodzajów mediów komunikacyjnych, możliwość funkcjonowania w ramach jednej sieci sterowania. Dzięki wbudowanym instrumentom umożliwia budowanie sieci urządzeń IzoT, z podłączeniem do dwóch kanałów Ethernet i do dwóch kanałów FT (para skręcona) lub RS-485. Router automatycznie przekazuje pakiety pomiędzy kanałami FT, Ethernet i RS-485. Każdy z jego interfejsów FT może zostać skonfigurowany do komunikacji z kanałem IzoT/FT lub LonTalk FT, otwierając drogę do ich integracji (współpraca klasycznych modułów automatyki budynkowej z węzłami IzoT). Router IzoT pełni może obsłużyć również kanały komunikacji standardu BACnet. Umożliwia to stacjom roboczym i urządzeniom BACnet/IP, przyłączonym do kanału IP (np. Ethernet), komunikację z urządzeniami BACnet/IP z wykorzystaniem kanału FT. Router IzoT wyposażony został w 4 porty USB, co rozszerza jego możliwości komunikacyjne, przez umożliwienie dołączenia dodatkowych interfejsów FT lub RS-485, a nawet adaptera Wi-Fi. Moduł routera posiada też zarządzane terminatory sygnału transmitowanego po każdym z przyłączanych kanałów FT. Oferuje obsługę protokołów i standardów wykorzystywanych w lokalnych (LAN) lub zewnętrznych (WAN) sieciach IP m.in. TCP, UDP, IPv4, IPv6, DHCP, DNS, FTP, ICMP, SNMP, SNTP, HTTP, HTTPS oraz SSL. Udostępnia interfejs RESTful API, wspierając XML i JSON, dla łatwego rozwoju stron internetowych i komunikacji M2M. Wspiera urządzenia, których aplikacje zostały rozwinięte dzięki IzoT Device Stack (Stos Urządzenia IzoT – opis w dalszej części raportu).

IzoT MCU's (Mikroprocesory IzoT) - dedykowane układy mikroprocesorowe dla platformy IzoT. Do grupy należą procesory Neuron 6050 oraz Smart Tranceivers FT 6050 i FT 6010.

Procesory Neuron 6050 zostały zaprojektowane jako podstawowe układy umożliwiające budowę i konsolidację nowoczesnych inteligentnych urządzeń sterujących. Stanowią one kluczowe elementy platformy IzoT, oferując możliwość kompatybilności wstecznej z platformą LonWorks oraz obsługę nowych kanałów komunikacyjnych platformy IzoT, poprzez dodanie natywnej obsługi sieci IP na poziomie urządzenia i konsolidację wielu protokołów sterowania w tym samym układzie. Procesory Neuron 6050 łączą funkcje komunikacji i sterowania, zarówno sprzętu jak i oprogramowania, w ramach jednego układu tak, aby ułatwić projektowanie urządzeń zgodnych z protokołami LonTalk, LonTalk/IP lub BACnet/IP. 5-pinowy port komunikacyjny procesora umożliwia jego skonfigurowanie do współpracy z szeroką gamą transceiverów, pracujących z różną szybkości transmisji danych, z wieloma rodzajami mediów transmisji np. pary skręconej (FT), radia (RF), podczerwieni (IR), światłowodu. Układ Neuron 6050 składa się z 3 niezależnych 8-bitowych procesorów logicznych dedykowanych do zarządzania warstwą fizyczną (procesor MAC), siecią (procesor NET) i aplikacją użytkownika (procesor APP) (patrz rys. 6) [26].



Rys. 6 – Architektura procesora Neuron 6050.

Dodatkowy czwarty procesor, odpowiadający za obsługę przerw (procesor IRQ), może być używany przy wyższych częstotliwościach zegara systemowego. Procesory Neuron 6050 cechują się wbudowanym zegarem systemowym osiągającym częstotliwości do 80 MHz, 64 KB pamięci RAM i 16 KB pamięci ROM, wsparciem zewnętrznej pamięci flash do 256 KB, obsługą 254 zmiennych sieciowych i 127 aliasów. Oferują możliwość obsługi programowalnych przez użytkownika przerw, sprzętowy UART, 12 wejść/wyjść z możliwością wyboru jednego z 35 predefiniowanych trybów pracy. Smart Tranceivers są układami typu SoC łączącymi w jednym układzie nadajnik i odbiornik oraz procesor. Do poprawnej komunikacji Smart Transceiver potrzebuje

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

specjalnego układu dopasowującego do medium komunikacyjnego – transformera. Powstał on z myślą o zredukowaniu kosztu budowy urządzeń. Układy FT6050 i FT6010 zawierają w sobie procesor Neuron z rodziny 6000, z wbudowaną obsługą stosów IP dla sieci sterowania oraz z transceiverem zapewniającym cztery interfejsy komunikacyjne LonTalk z kanałem FT, LonTalk/IP z kanałem FT, BACnet/IP z kanałem FT oraz dowolny protokół IP z kanałem FT. Elementem platformy IzoT są również narzędzia programistyczne: IzoT Network Services Server, IzoT Commissioning Tool oraz tzw. stosy IzoT Device Stack, IzoT Server Stack, umożliwiające programistom i inżynierom automatykom budowanie własnych urządzeń, modułów sieciowych, węzłów sieci IzoT, w oparciu o różne zasoby sprzętowe.

- IzoT Network Services Server (Serwer Usług Sieciowych) – platforma programistyczna przeznaczona dla projektowania, rozwijania, integrowania, monitorowania i sterowania aplikacji IzoT. Zapewnia usługi dla aplikacji systemów Windows, pozwalające na konfigurację urządzeń, połączeń, routerów i kanałów, a także podsystemów zawierających urządzenia i routery. Umożliwia tworzenie sieci IzoT lub LonWorks z maksymalną liczbą 32385 urządzeń w 1000 kanałów. Każde z urządzeń sieci może posiadać do 4096 punktów danych lub zmiennych sieciowych. Realizuje połączenia typu peer-to-peer pomiędzy urządzeniami lub między grupami urządzeń, wspiera wielo-kanałowość z wykorzystaniem routerów IzoT, LonWorks, IP-852 oraz różnych typów mediów transmisji danych Ethernet, Wi-Fi, RS-485, Power Line, para skręcona FT. Serwer działa ze wszystkimi urządzeniami IzoT i LonWorks, stanowiąc tym samym otwartą platformę obsługi wielu użytkowników prowadzących komisjonowanie węzłów sieci, monitorujących i obsługujących urządzenia oraz aplikacje pochodzące od różnych producentów i dostawców. Serwer utrzymuje informacje o wszystkich urządzeniach i o konfiguracji sieci w bazie danych o wysokiej wydajności. Sieci mogą być projektowane w trybie off-line, bez fizycznego dostępu do węzłów i kanałów sieciowych. Baza danych umożliwia zastępowanie uszkodzonych urządzeń w taki sposób, że konfiguracja i połączenia zostają automatycznie przenoszone do urządzenia zastępczego. Platforma zapewnia mechanizmy kopii zapasowej i przywracania baz danych oraz obsługi usług odczytu i zapisu punktów danych, zmiennych sieciowych i usług konfiguracyjnych
- IzoT Commissioning Tool (Narzędzie Integratorskie) – klasyczny pakiet integratorski przeznaczony do integrowania i komisjonowania urządzeń. Zapewnia obsługę wspomnianych operacji na urządzeniach w ramach projektu sieci sterowania, poprzez wykorzystanie interfejsu graficznego zaimplementowanego w pakiecie Microsoft Visio (podobnie jak w pakiecie LonMaker, do integracji sieci automatyki budynkowej standardu LonWorks). Zachowano zatem spójność platformy programistycznej dla integratorów sieci automatyki budynkowej, również z elementami nowego rozwiązania IzoT. Podczas wykonywania projektu sieci pakiet komunikuje się z urządzeniami, aby dopasować je do powstającej w programie reprezentacji graficznej. Zapewnienie komunikacji i wymiany informacji pomiędzy urządzeniami realizowane jest w projekcie przez połączenie linią na rysunku topologii odpowiednich punktów danych. Rezultatem integracji sieci jest jej graficzna reprezentacja w projekcie, która wykorzystywana jest również jako element dokumentacji technicznej i powykonawczej. Narzędzie współpracuje ze wszystkimi urządzeniami IzoT i LonWorks pochodzącymi od różnych producentów oraz różnymi typami mediów transmisji danych Ethernet, Wi-Fi, RS-485, Power Line, para skręcona. Zawiera mechanizmy zarządzania siecią sterowania zaimplementowane w platformie IzoT Network Services Server (Serwer Usług Sieciowych). Wspiera aplikacje typu plug-in przeznaczone dla IzoT, OpenLNS i LNS. Oferuje mechanizmy importowania i eksportowania danych do/z plików XML oraz rysunków

projektów sieci do/z programu AutoCAD. Zawiera również narzędzie przeglądarki zmiennych sieciowych urządzeń wykorzystanych w ramach projektu.

- IzoT Device Stack (Stos Urządzenia IzoT) – kod źródłowy jednostek MCU urządzeń protokołu IzoT. Umożliwia deweloperom/programistom budowę urządzeń komunikujących się w ramach sieci IzoT, zgodnej z ideą Przemysłowego Internetu Rzeczy (IIoT), z wykorzystaniem 16, 32 lub 64-bitowego procesora i systemu operacyjnego. Wykorzystanie Device Stack pozwala na szybką i łatwą wymianę danych między urządzeniami, z wykorzystaniem modelu publish-subscribe danych poprzez kanał IP. Urządzenia mogą zbierać dane z czujników do monitorowania parametrów fizycznych (takich jak temperatura, wilgotność, poziom zużycia energii, itd.) a następnie udostępnić je innym modułom IzoT. Dane otrzymane z innych urządzeń/węzłów sieci IzoT lub lokalnych czujników, mogą z kolei zostać wykorzystane do sterowania elementów wykonawczych (takich jak ściemniacze LED, siłowniki, przepustnice, elektromagnesy, itd.). Wszystkie informacje i parametry mogą być monitorowane oraz kontrolowane za pośrednictwem stron internetowych, jednocześnie ze wszystkich urządzeń IzoT, z wykorzystaniem IzoT Serwerów. IzoT Device Stack zawiera IzoT Python Package (Pakiet Python IzoT), który pozwala na rozwijanie aplikacji urządzeń w języku programowania Python 3. Pakiet ten ułatwia deweloperom aplikacji określenie punktów danych wejściowych i wyjściowych, w relacji z innymi urządzeniami IzoT w lokalnych sieciach sterowania w taki sposób, że urządzenie informuje i jest informowane o wszystkich zmiennych sieciowych. Jedną ze znaczących cech platformy IzoT jest zdolność do łatwego tworzenia grup współdziałających urządzeń, dzięki mechanizmowi ISI (Interoperable Self-Installation), zaimplementowanemu w stosie IzoT Device Stack. Mechanizm ten, wykorzystując podstawową ideę urządzeń IzoT, pozwala od razu po podłączeniu od lokalnej sieci IP modułu IzoT na poinformowanie o tym fakcie innych węzłów sieci i uzyskanie informacji o dostępnych punktach danych, a następnie automatyczną rekonfigurację siatki połączeń, w celu zapewnienia optymalnej efektywności wymiany danych. Proces ten odbywa się bez dodatkowych narzędzi integratorskich lub serwerów [27].

- IzoT Server Stack (Stos Serwera IzoT) - kod źródłowy pozwalający programistom na tworzenie aplikacji serwera sieci Web dla platformy Izo, który działa z 32-bitowym procesorem i systemem operacyjnym. Serwery zbudowane z wykorzystaniem IzoT Server Stack umożliwiają podłączenie urządzeń IzoT do klientów sieci Internet, zapewniając użytkownikom dostęp do monitorowania i sterowania urządzeń w ramach lokalnych sieci. Stos oferuje łatwy w użyciu interfejs RESTful API wraz z interfejsem dla wyszukiwania urządzeń w sieci, monitorowania ich danych i sterowania nimi za pośrednictwem wejść sieciowych. Platforma IzoT umożliwia programistom tworzenie grup (społeczności) współdziałających urządzeń. Możliwe jest zatem wykorzystanie jej jako podstawy budowy wspomnianych już wcześniej w raporcie tzw. smart społeczności, opartych na poziomie obiektowym o zintegrowane na poziomie budynku/domu grupy urządzeń [15]. IzoT Server Stack automatycznie wykrywa urządzenia podłączone do lokalnej sieci sterowania za pomocą mechanizmu ISI, zaimplementowanego w IzoT Device Stack. Usługi REST zaimplementowane w stosie, umożliwiają każdej stronie internetowej lub aplikacji uzyskanie listy urządzeń wykrytych przez serwer, określenie punktów danych, które są publikowane przez urządzenia oraz zdefiniowanie odpowiednich postaci sygnałów wejściowych, w celu sterowania i operowania modułami. IzoT Server Stack monitoruje raz wykryte i widoczne punkty danych, poprzez utrzymanie ciągle aktualnych wartości zmiennych sieciowych w bazie danych. Każdy z klientów sieci może korzystać z interfejsu IzoT REST API, aby uzyskać informacje z aktualną wartością wszelkich punktów danych w bazie danych stosu

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

IzoT Serwera. Interfejs umożliwia także aktualizowanie punktów danych wejściowych urządzeń lokalnej sieci sterowania. Korzystanie z usług punktów danych interfejsu IzoT REST API, daje użytkownikom możliwość tworzenia w prosty sposób strony sieci Web do wyświetlania danych otrzymanych z urządzeń IzoT oraz do ich sterowania [20][28]. Oba stopy IzoT (stocks) zostały udostępnione w postaci kodu źródłowego dla popularnej platformy sprzętowej Raspberry Pi. Kod ten może zostać „przeportowany”, przeniesiony do różnych 32-bitowych procesorów i systemów operacyjnych.

7. IoT jako platforma integracji funkcjonalnej w automatyce budynkowej

Obecnie w monitoringu i sterowaniu wielu branżowych podsystemów infrastruktury budynków, coraz powszechniejsze jest stosowanie systemów automatyki bazujących na sieciach magistralnych – tzw. sieci obiektowych (Fieldbus Area Network). Jednak w przeciągu ostatnich trzech dekad na rynku automatyki budynkowej pojawiło się wiele różnych protokołów dedykowanych do sieci tego typu, gdy tymczasem, z punktu widzenia integracji systemowej i funkcjonalnej, najbardziej pożądane byłoby istnienie jednolitego standardu obsługującego wszystkie urządzenia wykonawcze, czujniki, sterowniki itp. W praktyce instalacyjnej istnieją zatem heterogeniczne struktury sieci różnych standardów, które utrudniają integrację platform sterowania i monitoringu oraz bardziej efektywne zarządzanie budynkami. Wprowadzenie technologii Internetu Rzeczy, wraz z protokołem IPv6, wydaje się idealnym rozwiązaniem i narzędziem do stopniowego włączenia tych struktur w ramy sieci teleinformatycznych. Skutkiem tych działań, w najbliższych kilku latach, coraz powszechniejsze będą homogeniczne sieci automatyki, sterowania i monitoringu. Generuje to jednak szereg wyzwań z którymi muszą zmierzyć się zarówno sami integratorzy systemowi jak i technolodzy, zaangażowani w rozwój lokalnych i nadrzędnych systemów sieciowych. Na rynku systematycznie pojawiają się nowe rozwiązania, oparte o protokół IP i dedykowane do obsługi zróżnicowanych pod względem funkcjonalnym i peryferyjnym węzłów sieciowych [5] (patrz: rozdział 1 raportu).

Drugą, niemniej istotną kwestią jest koncepcja organizacji funkcjonalnej, logicznej tego typu systemów. Idea integracji wymaga bowiem nie tylko ujednoczenia technologii i protokołu komunikacji, ale również wypracowania standardów w zakresie realizowanych funkcji – zarówno dla pojedynczych urządzeń, jak i modułów realizujących wzajemnie różne funkcje. Architektura oprogramowania zawarta w protokołach standardów sieci obiektowych automatyki budynkowej i przemysłowej wykorzystuje komponenty, które są zdefiniowane za pomocą ustandaryzowanych profili. Profile te definiują funkcje aplikacji urządzeń dla danego systemu automatyki, wraz z niezbędnymi obiektami komunikacji (zmiennie sieciowe). Jednak zwykle brak jest w nich informacji dotyczących możliwej współpracy urządzeń i ich aplikacji z różnych branż, podsystemów budynków. Dlatego też w praktyce instalacyjnej i integratorskiej, wiele grup roboczych zajmujących się rozwojem i implementacją obiektowych sieci sterowania, niejednokrotnie zetknęło się z problemami wynikającymi z konieczności zastosowania konkretnych, zdefiniowanych profili funkcjonalnych w większych systemach. Problemy te dotyczą podejścia do kompleksowej organizacji funkcjonalnej całej, zintegrowanej

sieci sterowania, składającej się z wielu podsystemów, a w nich urządzeń zgodnych z poszczególnymi profilami funkcjonalnymi.

Problem ten nabiera szczególnego znaczenia w perspektywie wdrożenia idei Internetu Rzeczy (IoT) oraz zastosowania w budynkach bardzo dużej liczby „inteligentnych” czujników czy elementów wykonawczych (Smart Obiekty, jako nowoczesne czujniki, elementy wykonawcze itp.). W takich systemach nie jest konieczne stosowanie dodatkowych sterowników lub koncentratorów sygnałów (np. moduły wejść/wyjść), a węzły sieci, nawet niewielkie, mogą działać autonomicznie, lub wymieniać dane z innymi węzłami, przez kanały IP. Dlatego konieczne jest rozważanie redefinicji lub zmiany koncepcji podejścia do profili funkcjonalnych tak, aby ułatwić proces projektowania i integracji urządzeń w ramach systemów automatyki budynkowej zrealizowanych za pomocą IoT [29]. Nabiera ono szczególnego znaczenia w perspektywie zastosowanie mechanizmów ISI (Interoperable Self-Installation), ułatwiających integrację oraz autointegrację urządzeń w sieci automatyki lub zastosowanie mechanizmów sztucznej inteligencji (AI) w celu autoorganizacji sieci sterowania (urządzenia włączane do sieci same wykrywają inne urządzenia w niej działające i konfiguruje podstawowe połączenia funkcjonalne z nimi). Dotychczasowe podejście oparte o standardowe profile funkcjonalne, jeśli w ogóle wskazuje, opisuje tylko w sposób niejawni relacje między poszczególnymi profilami i dostępnymi w nich zmiennymi sieciowymi. Proponowana przez autorów niniejszego raportu zmiana sposobu podejścia do organizacji funkcjonalnej sieciowych systemów automatyki i, monitoringu i zarządzania, powinna uwzględniać również relacje pomiędzy profilami i wynikające z nich determinanty tworzenia struktury sieci, ponieważ realizacja systemu automatyzacji i sterowania budynkiem wymaga rzetelnej identyfikacji funkcjonalności znajdujących się w nim instalacji technologicznych, funkcji pomieszczeń oraz analizy funkcji systemu automatyki i wyposażenia technicznego. Każde urządzenie powinno podlegać dokładnie ustalonym regułom działania, na których inne urządzenia w sieci sterowania mogłyby polegać. Tylko w ten sposób możliwe jest zagwarantowanie spójnego "obrazu systemu", ustandaryzowanej i elastycznej zarazem platformy wymiany informacji i realizacji zaawansowanych funkcji sterowania i zarządzania infrastrukturą budynkową. Istotę i złożoność problemu jednolitej, funkcjonalnej integracji węzłów sieci rozproszonej można zobrazować na przykładzie organizacji stosunkowo prostego i podstawowego scenariusza sterowania, zakładającego automatyczne załączenie oświetlenia w pomieszczeniu w przypadku zbyt niskiego poziomu natężenia światła. W przykładzie zostanie podane rozwiązanie bazujące na profilach funkcjonalnych standardu LonWorks oraz realizacji za ich pomocą określonej funkcjonalności. W takim przypadku wymagane jest zastosowanie odpowiednich strategii sterowania:

- Strategia odpowiadająca za pracę lampy w standardzie LonWorks opisana jest za pomocą profilu nr #3040_10. Profil elementu wykonawczego lampy (#3040_10) jest przeznaczony dla węzłów sieci sterujących poziomem iluminacji oprawy oświetleniowej [30]. Typowymi elementami lampy wykonawczej są ściemniacze, przekaźniki oraz elektronicznie regulowane balasty. Profil ten obowiązkowo przewiduje zastosowanie zmiennych sieciowych odpowiadających za: odebranie z sieci sterowania rozkazu załączenia/wyłączenia elementu wykonawczego oraz dostarczanie informacji o stanie pracy i poziomie iluminacji. Szczegółowo definiuje on dwie wymagane zmienne sieciowe typu SNVT_switch o nazwach: nvlLampValue (zadawanie rozkazu) i nvoLampValueFb (realizacja sprzężenia zwrotnego od stanu pracy i poziomu iluminacji). Opcjonalnie w profilu przewidziano zmienne dostarczające informacje o ilości godzin pracy wraz ze zgłoszeniem alarmu czasu pracy oraz wartość zużytej energii przez lampę. Dodatkowo zdefiniowano właściwości konfiguracyjne

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

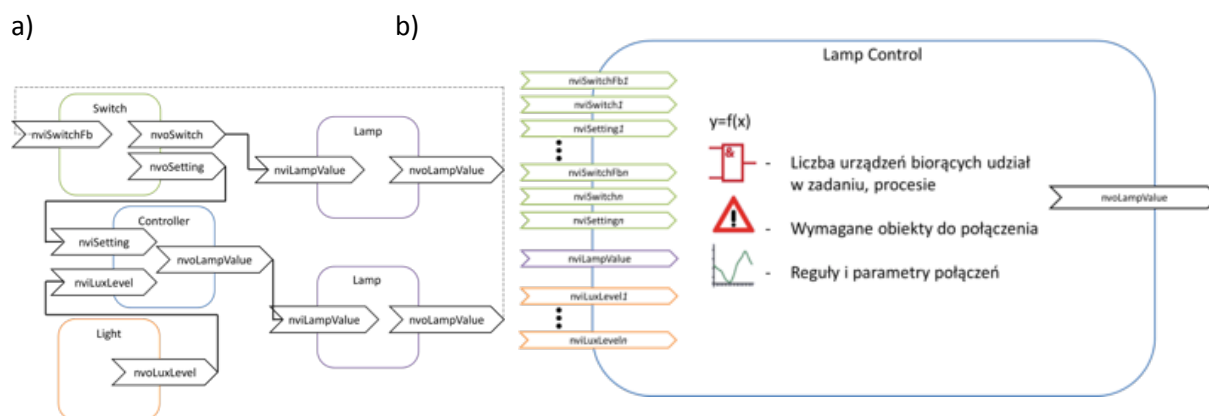
umożliwiająca ustawienie tekstu identyfikującego lokalizację zainstalowanej lampy, opóźnienie pomiędzy aktualizacją zmiennej `nviLampValue` a aktualizacją zmiennej `nvoLampValueFb`, stan załączenia oświetlenia po włączeniu węzła sieci, ustawienie wstępnej oraz alarmowej wartości całkowitego czasu pracy oraz zużytej energii elektrycznej. Po przekroczeniu wartości alarmowej węzeł sieci ma zgłosić taką informację z wykorzystaniem zmiennej statusu bloku obiektu węzła. W specyfikacji profilu podano znaczenie, prawidłowy zakres, warunki transmisji oraz domyślny typ usługi transmisji tych zmiennych i właściwości konfiguracyjnych. Typowe zastosowanie urządzeń zgodnych z tym profilem, w ramach scenariusza sterowania, to połączenie z modułami włącznika i sterownika (sterownik stałego natężenia oświetlenia, sterownik scen świetlnych).

- Strategia odpowiadająca za pracę czujnika natężenia oświetlenia w standardzie LonWorks opisana jest za pomocą profilu nr #1010_11. Profil czujnika #1010_11 jest przeznaczony dla węzłów sieci, które odpowiedzialne są za pomiar poziomu natężenia oświetlenia [30]. Profil ten obowiązkowo przewiduje zastosowanie zmiennej sieciowej odpowiadającej za transmitowanie do sieci sterowania o aktualnie panującym poziomie natężenia oświetlenia. Opcjonalnie w profilu przewidziano właściwości konfiguracyjne umożliwiające ustawienie tekstu identyfikującego lokalizację zainstalowanego czujnika, ustawienie współczynnika odbicia światła, wartość natężenia światła uwzględnianą podczas procesu autokalibracji, interwały czasowe odnośnie transmisji zmierzonej wartości do sieci sterowania. Typowe zastosowanie urządzeń zgodnych z tym profilem, w ramach scenariusza sterowania, to połączenie z modułami sterownik stałego natężenia oświetlenia.

- Strategia odpowiadająca za pracę sterownika stałego natężenia oświetlenia w standardzie LonWorks opisana jest za pomocą profilu nr #3050_10 [30]. Profil ten obowiązkowo przewiduje zastosowanie zmiennych sieciowych odpowiadających za: odebranie z sieci sterowania informacji o aktualnie panującym poziomie natężenia oświetlenia (`nviLuxLevel`), odebranie rozkazu o trybie pracy sterownika i wartości punktu nastawy (`nviSetting`), wysłanie rozkazu, zawierającego obliczony na podstawie posiadanych przez sterownik informacji, o trybie pracy i poziomie natężenia iluminacji lampy. Obowiązkowo zdefiniowano również właściwość konfiguracyjną odpowiedzialną za ustawienie punktu nastawy poziomu natężenia oświetlenia jaki zapewnić ma sterownik. Opcjonalnie w profilu przewidziano zmienną sieciową przyjmującą informacje o ręcznie i/lub nadrzędnie zadanym punkcie nastawy. Ustawienie zmiennej spowoduje, że rozkaz o stanie pracy lampy wprowadzony na wejście sterownik bezpośrednio jest przekazywany na jego wyjście. Dodatkowo zdefiniowano właściwości konfiguracyjne umożliwiające ustawienie tekstu identyfikującego lokalizację zainstalowanego sterownika, interwały czasowe odnośnie transmisji zmierzonej wartości do sieci sterowania, wartości opóźnienia załączenia/wyłączenia jeśli poziom natężenia oświetlenia odpowiednio jest zbyt niski/wysoki oraz stan pracy sterownika po włączeniu węzła sieci.

A zatem przy obowiązującej obecnie metodzie realizacji zakładanego na wstępie scenariusza sterowania konieczne jest zastosowanie strategii definiujących zachowanie oraz funkcjonalności poszczególnych urządzeń, instalacji technologicznych czy modułów automatyki. Na podstawie tych informacji integrator proponuje i opracowuje każdorazowo strukturę ich wzajemnych połączeń fizycznych, a przede wszystkim logicznych. W niektórych opracowaniach naukowych i branżowych profile funkcjonalne w takiej postaci określane są nawet mianem 8 warstwy protokołu IOS/OSI, dedykowanego dla sieci obiektowych [31].

Tymczasem w nowoczesnych systemach automatyki budynkowej, mnogość integrowanych podsystemów i urządzeń infrastruktury budynków domaga się wprowadzenia ujednoczonych profili zadaniowych (schematów funkcjonalnych), dedykowanych do obsługi określonych funkcji, zadań realizowanych w układach złożonych z wielu urządzeń, czujników, sterowników itd. Próby formułowania wytycznych dla takich schematów podejmowano już w dyskusjach naukowo-branżowych, jednak jak dotąd nie zostały one wdrożone [29]. W perspektywie implementacji na poziomie sieci obiektowych rozwiązań technologii IoT, autorzy raportu proponują powrót do tych koncepcji i opracowanie w dalszych etapach prac badawczych, szczegółowych wytycznych dla takich właśnie schematów funkcjonalnych. Na rysunku 7 pokazano schematycznie różnicę w podejściu opartym o klasyczne profile i bloki funkcjonalne standardu LonWorks, a proponowanej koncepcji schematów, profili zadaniowych – w odniesieniu do opisanego wcześniej przykładu aplikacji automatycznego załączenia oświetlenia w pomieszczeniu, w przypadku zbyt niskiego poziomu natężenia światła.



Rys. 7 – Struktury połączeń logicznych w przykładowej aplikacji sterowania oświetleniem: . a) model klasyczny w oparciu o profile funkcjonalne, b) proponowany profil zadaniowy

8. Wytyczne do utworzenia laboratorium badawczego nowoczesnych technologii Internetu Rzeczy integrowanych z systemami automatyki budynkowej

Jak wskazują wyniki przeprowadzonych analiz, technologia Internetu Rzeczy staje się integralnym elementem współczesnych systemów automatyzacji, monitoringu i sterowania w budynkach. Dlatego też, w celu poszerzenia zdolności poznawczych, umożliwienia realizacji dalszych prac badawczo-rozwojowych Internetu Rzeczy w szeroko pojętych zastosowaniach związanych z automatyką budynkową, celem jest określenie pewnych wytycznych umożliwiających utworzenie odpowiednich do tego celu stanowisk laboratoryjnych i dydaktycznych.

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

Stanowiska takie powinny zostać wyposażone odpowiednio w niezbędną infrastrukturę sprzętową oraz oprogramowanie.

Niezbędna infrastruktura sprzętowa:

1. Zestawy uruchomieniowe – platformy sprzętowo-programistyczne dla systemów wbudowanych, umożliwiające szybkie prototypowanie i implementację nowych urządzeń automatyki budynkowej zgodnych z ideą IoT
 - a. Arduino – projekt, oparty o ideę open hardware - referencyjny schemat sprzętowy układu Arduino jest rozpowszechniany na licencji Creative Commons. Oferuje dużą liczbę wersji układów różniących się zastosowanym procesorem, wymiarami, zastosowanymi peryferiami i interfejsami komunikacyjnymi. W ramach projektu powstał język programowania Arduino (oparty na środowisku Wiring i zasadniczo na języku C/C++), a programowanie odbywa się najczęściej za pośrednictwem Arduino IDE - udostępniane i rozpowszechniane na licencji GPLv2. Jedną z największych zalet projektu jest jego dość znacząca popularność w środowisku branżowym (społeczność blogerów, fora Internetowe) oraz duża ilość opracowanych dodatków sprzętowych i klonów platformy. Płyty rozszerzeń wzbogacają bazowe układy Arduino o różnorodne funkcje jak: interfejs Ethernet lub Bluetooth, kontrolę silników itp. Przykładowe płyty to: Arduino Ethernet Shield, Arduino Motor Shield, XBee Shield, TouchShield, Extender Shield, InputShield
 - b. Raspberry - platforma komputerowa oparta na układzie Broadcom BCM2835 SoC, który składa się z procesora ARM1176JZF-S 700 MHz, VideoCore IV GPU i 256 lub 512 MB pamięci RAM. Urządzenie nie posiada dysku twardego, ale w celu załadowania systemu operacyjnego i przechowywania danych, oferuje złącze dla kart SD. Urządzenie działa pod kontrolą systemów operacyjnych opartych na Linuksie oraz RISC OS. Raspberry Pi posiada podstawowe interfejsy komunikacyjne takie jak: złącze USB – do podłączenia dowolnych urządzeń zewnętrznych w tym adapterów Wi-Fi (bezprzewodowej karty sieciowej), gniazdo Ethernet – umożliwiające bezpośrednie podłączenie do sieci LAN. Dodatkowe interfejsy to GPIO - wyjścia/wejścia ogólnego przeznaczenia, mogą służyć do obsługi diod LED, przycisków, sterowników silników, magistrala I2C - umożliwiająca komunikację z różnego rodzaju czujnikami (np. temperatury czy przyspieszenia), SPI - pozwalający podłączyć szybkie przetworniki analogowo/cyfrowe oraz różnego rodzaju pamięci, UART - popularny, prosty interfejs szeregowy. Platforma Raspberry Pi posiada bogatą ofertę modułów dodatkowych i płyt rozszerzających takich jak dedykowana kamera, wyświetlacz dotykowy oraz płyty rozszerzające PiFace, Gertboard, PiRack, ProtoPi, itd.
 - c. FT 6000 EVK – zestaw sprzętowy wraz z dedykowanym oprogramowaniem dla sieci LonWorks i platformy IzoT. Umożliwia on rozwój urządzeń i ich aplikacji pracujących w technologii LonWorks, LonWorks/IP oraz BACnet/IP. Zawiera dwie płytki uruchomieniowe zawierające podstawowe układy sprzętowe jak wejścia/wyjścia, wyświetlacz LCD itp., umożliwiające szybkie prototypowanie urządzeń systemów automatyki budynkowej. W składzie zestawu znajduje się również router IzoT, zawierający kanały FT i Ethernet, umożliwiający rozwój aplikacji niezbędnych do obsługi, zarządzania i monitorowania urządzeń IoT.
2. Podstawowe elementy elektryczne i elektroniczne - służące do budowy urządzeń IoT.
 - a. Sensory, czujniki - np. elementy elektroniczne (analogowe, cyfrowe) umożliwiające pomiar podstawowych parametrów środowiskowych (temperatura, natężenie oświetlenia, ruch, itd.), układy pomiarowe prądu i napięcia.

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl isi@agh.edu.pl

- b. Elementy wykonawcze - podstawowe elementy elektroniczne np. przekaźniki, silniki, diody itp.
- c. Płytki prototypowe i uniwersalne oraz niezbędny osprzęt elektryczne jak kable, przewody itp.
- 3. Infrastruktura sieciowa - niezbędna do tworzenia sieci komunikacyjnych oraz sterowania.
 - a. routery, switchy IP - urządzenia sieciowe służące do łączenia różnych sieci komputerowych, umożliwiające zarządzanie ruchem.
 - b. routery, switchy, bramki, serwery automatyki dla poszczególnych standardów automatyki - możliwość budowy infrastruktury sieci sterowania automatyki budynków. Urządzenia te często pozwalają na łączenie ze sobą różnych mediów transmisji danych.
- 4. Moduły i interfejsy popularnych systemów automatyki budynków - niezbędne w celu badania integracji systemów i ich urządzeń dla poszczególnych standardów automatyki budynkowej i sieci IoT. Przykładowo: moduły wejść/wyjść, moduły czujników wielkości fizycznych, moduły wykonawcze.
- 5. Komputer klasy PC - niezbędny do uruchomienia odpowiednich środowisk programowych, narzędzi obsługi platform sprzętowych i integracyjnych automatyki budynkowej oraz technologii IoT. Ponadto do tworzenia aplikacji na urządzenia, integracji sieci sterowania oraz zarządzania, sterowania i monitorowania.

Niezbędna infrastruktura programowa:

- 1. Środowiska programistyczne IDE – np. PyCharm 3 - środowisko programistyczne języka Python. Oferuje obsługę biblioteki standardowej języka Python, graficzny debugger, inteligentny edytor kodu (kolorowanie składni, auto-upełnianie i -formatowanie), refaktoring i inspekcję kodu, wsparcie dla virtualenv/buildout, wsparcie dla bibliotek PyQt i PyGTK, wbudowany lokalny terminal, integrację z repozytorium (tj. mercurial, svn, git, cvs) czy menadżer projektów i pakietów.
- 2. Node-RED – nowoczesne narzędzie służące do łączenia modułów sprzętowych, ich aplikacji sterowania oraz usług sieciowych. Udostępnia ono zarządzany przez przeglądarkę edytor przepływu danych, który umożliwia łatwe łączenie elementów aplikacji funkcjonalnych urządzeń i modułów sieci, w ramach tzw. węzłów. Edytor umożliwia również tworzenie funkcji JavaScript, z wykorzystaniem bogatych możliwości wbudowanego Eclipse Orion. Oprogramowanie to zostało przygotowane do pracy z różnymi platformami sprzętowymi jak Arduino, Raspberry itd.
- 3. Oprogramowanie komputerowe do wspomaganie projektowania obwodów drukowanych PCB np. Eagle, które zawiera edytor schematów i płytek drukowanych.
- 4. Visual Control - oprogramowanie dla systemów operacyjnych MS Windows XP/7/8, które znacznie upraszcza i przyspiesza proces budowy i zarządza sieciami automatyki budynków. Pozwala na graficzne tworzenie aplikacji urządzeń, ładowanie ich do węzłów sieciowych oraz łączenie zmiennych sieciowych.
- 5. Wireshark – Wykorzystywany do przechwytywania, analizowania, charakteryzowania i wyświetlania pakietów sieciowych. Umożliwia on na ich podstawie zidentyfikowanie błędów zarówno powstających w strukturze sieci, jak i w urządzeniach sieciowych. Ułatwia prowadzenie diagnostyki i prac serwisowych integratorów sieci, poprzez wskazanie możliwych rozwiązań.

Bibliografia:

- [1] T. Sánchez López, D. C. Ranasinghe, M. Harrison, and D. McFarlane, "Adding sense to the Internet of Things," *Pers. Ubiquitous Comput.*, vol. 16, no. 3, pp. 291–308, Jun. 2011.
- [2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.
- [3] O. Vermesan and P. Friess, *The Internet of Things. Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers, 2013.
- [4] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *IEEE Internet Comput.*, vol. 14, no. 1, pp. 44–51, Jan. 2010.
- [5] D. Hutchison, A. Galis, and A. Gavras, *The Future Internet - LNCS 7858*. SPRINGER Open, 2013.
- [6] O. Hersent, D. Boswarthick, and O. Elloumi, *The Internet of Things. Applications to the Smatr Grid and Building Automation*. A John Wiley & Sons, Ltd., 2012.
- [7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.
- [8] A. Brachman, "Internet przedmiotów," 2013.
- [9] A. J. Jara, P. Moreno-Sanchez, A. F. Skarmeta, S. Varakliotis, and P. Kirstein, "IPv6 addressing proxy: mapping native addressing from legacy technologies and devices to the Internet of Things (IPv6).," *Sensors (Basel)*, vol. 13, no. 5, pp. 6687–712, Jan. 2013.
- [10] M. Jung, J. Weidinger, W. Kastner, and A. Olivieri, "Building Automation and Smart Cities: An Integration Approach Based on a Service-Oriented Architecture," in *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, 2013, pp. 1361–1367.
- [11] M. Jung, J. Weidinger, C. Reinisch, W. Kastner, C. Crettaz, A. Olivieri, and Y. Bocchi, "A Transparent IPv6 Multi-protocol Gateway to Integrate Building Automation Systems in the Internet of Things," in *2012 IEEE International Conference on Green Computing and Communications*, 2012, pp. 225–233.
- [12] F. Carrez, M. Bauer, M. Boussard, and N. Bui, "Internet of Things - Architecture IoT - A Final architectural reference model for the IoT v3 . 0," 2013.
- [13] J. Young, "BIoT BUILDING Internet of Things," *AutomatedBuildings.com*. [Online]. Available: <http://www.automatedbuildings.com/news/mar14/articles/realcomm/140219043909realcomm.html>.
- [14] Memoori, "Building Automation Prepares for the Building Internet of Things (BIoT)," *Memoori.com*.
- [15] X. Li, R. Lu, X. Liang, and X. S. Shen, "Smart Community : An Internet of Things Application," *IEEE Commun. Mag.*, no. November, pp. 68–75, 2011.
- [16] J. Byun, I. Hong, B. Kang, and S. Park, "A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting," *IEEE Trans. Consum. Electron.*, vol. 57, no. 2, pp. 436–444, May 2011.
- [17] A. OŻADOWICZ, "Zarządzać energią z głową : OpenADR – dwukierunkowa komunikacja dostawcy energii–odbiorcy," *Energetyka Ciepłna i Zawodowa*, pp. 109–112, 2013.
- [18] N. Bui, A. P. Castellani, P. Casari, and M. Zorzi, "The Internet of Energy :," *IEEE Netw.*, no. August, pp. 39–45, 2012.

- [19] O. Monnier, "A smarter grid with the Internet of Things," *Texas Instruments White Paper*, 2013
- [20] S. Ramakrishnan and S. Ramakrishnan, "WoT (Web of Things) for Energy Management in a Smart Grid-Connected Home," *Issues Informing Sci. Inf. Technol.*, vol. 10, 2013.
- [21] D. Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," *CISCO White Paper*, no. April, 2011.
- [22] S. Ferber, "How the Internet of Things Changes Everything," *Harvard Business Review Blog*, 2013. .
- [23] W. Kastner, G. Neugschwandtner, S. Soucek, and H. M. Newman, "Communication Systems for Building Automation and Control," vol. 93, no. 6, 2005.
- [24] I. G. Hamilton, A. J. Summerfield, R. Lowe, P. Ruyssevelt, C. a. Elwell, and T. Oreszczyn, "Energy epidemiology: a new approach to end-use energy demand research," *Build. Res. Inf.*, vol. 41, no. 4, pp. 482–497, Aug. 2013.
- [25] Echelon Corp., "IzoT™ Platform Info," *WWW page*, 2014. .
- [26] Echelon Corp., "Series 6000 Chip Data," *datasheet*, 2014. .
- [27] Echelon Corp., "IzoT Device Stack," *datasheet*, 2013. .
- [28] Echelon Corp., "IzoT Server Stack," *datasheet*, 2014. .
- [29] K. Kabitzsch and G. Stain, "NETWORK PROFILES FOR LON," 2000.
- [30] LonMark, "Standard Program Identifier (SPID) Master List," 2014. [Online]. Available: https://www.lonmark.org/technical_resources/resource_files/spid_master_list#DeviceClasses.
- [31] G. Pratl, D. Dietrich, G. P. Hancke, and W. T. Penzhorn, "A New Model for Autonomous , Networked Control Systems," *IEEE Trans. Ind. Informatics*, vol. 3, no. 1, pp. 21–32, 2007.