TECHNOLOGY IN ACTION™

Komercyjne i przemysłowe aplikacje Internetu rzeczy na Raspberry Pi

Prototypowanie rozwiązań IoT

Ioana Culic
Alexandru Radovici
Cristian Rusu

Apress®

Apress®

Ioana Culic
Alexandru Radovici
Cristian Rusu

Komercyjne i przemysłowe aplikacje Internetu rzeczy na Raspberry Pi

Prototypowanie rozwiązań IoT

Przekład: Maria Chaniewska

APN Promise, Warszawa 2020

Komercyjne i przemysłowe aplikacje Internetu rzeczy na Raspberry Pi. Prototypowanie rozwiązań IoT

First published in English under the title
Commercial and Industrial Internet of Things Applications with the Raspberry Pi: Prototyping IoT Solutions by Ioana Culic, Alexandru Radovici, Cristian Rusu

Copyright © 2020 by Ioana Culic, Alexandru Radovici, Cristian Rusu

This edition has been translated and published under licence from APress Media, LLC, part of Springer Nature.

APress Media, LLC, part of Springer Nature takes no responsibility and shall not be made liable for the accuracy of the translation.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from publisher.

Polish language edition published by APN PROMISE S.A., Copyright © 2020

Autoryzowany przekład z wydania w języku angielskim, zatytułowanego: Commercial and Industrial Internet of Things Applications with the Raspberry Pi: Prototyping IoT Solutions by Ioana Culic, Alexandru Radovici, Cristian Rusu, opublikowanego przez APress Media, LLC, oddział Springer Nature.

Wszystkie prawa zastrzeżone. Żadna część niniejszej książki nie może być powielana ani rozpowszechniana w jakiejkolwiek formie i w jakikolwiek sposób (elektroniczny, mechaniczny), włącznie z fotokopiowaniem, nagrywaniem na taśmy lub przy użyciu innych systemów bez pisemnej zgody wydawcy.

APN PROMISE SA, ul. Domaniewska 44a, 02-672 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: wydawnictwo@promise.pl

Książka ta przedstawia poglądy i opinie autorów. Przykłady firm, produktów, osób i wydarzeń opisane w niniejszej książce są fikcyjne i nie odnoszą się do żadnych konkretnych firm, produktów, osób i wydarzeń, chyba że zostanie jednoznacznie stwierdzone, że jest inaczej. Ewentualne podobieństwo do jakiejkolwiek rzeczywistej firmy, organizacji, produktu, nazwy domeny, adresu poczty elektronicznej, logo, osoby, miejsca lub zdarzenia jest przypadkowe i niezamierzone.

Wszystkie znaki towarowe występujące w książce mogą być własnością ich odnośnych właścicieli.

APN PROMISE SA dołożyła wszelkich starań, aby zapewnić najwyższą jakość tej publikacji. Jednakże nikomu nie udziela się rękojmi ani gwarancji.
APN PROMISE SA nie jest w żadnym wypadku odpowiedzialna za jakiekolwiek szkody będące następstwem korzystania z informacji zawartych w niniejszej publikacji, nawet jeśli APN PROMISE została powiadomiona o możliwości wystąpienia szkód.

ISBN: 978-83-7541-430-1 (druk), 978-83-7541-439-4 (ebook)

Przekład: Maria Chaniewska
Redakcja: Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Spis treści

O autorach ix
O recenzencie technicznym x
Wstęp xi

Rozdział 1. **Przegląd systemów IoT** 1
Co to jest przemysłowy Internet rzeczy? 1
Cechy IoT 3
Architektura IoT 5
Systemy IIoT 7
System SCADA 8
Od prototypowania do systemów przemysłowych 10
Szczególne cechy IIoT 12
Przetwarzanie brzegowe 13
Raspberry Pi jako urządzenie brzegowe 15
Raspberry Pi w przemyśle 16
Protokoły komunikacyjne IoT 18
Niskopoziomowe protokoły transmisji danych 19
Protokoły poziomu aplikacji 22
Interfejs z systemem IoT 24
Interfejs użytkownika 24
Fizyczne elementy sterujące 26
Interfejs platformy 26
Oprogramowanie systemów IoT 27
Cechy oprogramowania 28
Wytwarzanie oprogramowania 29
Podsumowanie 33
Dalsza literatura 34

Rozdział 2. Wprowadzenie do Raspberry Pi oraz Wyliodrin STUDIO 37

Opis Raspberry Pi 38
Opis Wyliodrin STUDIO 41
Uruchamianie Wyliodrin STUDIO 42
Uruchamianie Wyliodrin STUDIO lokalnie 42
Uruchamianie Wyliodrin STUDIO w przeglądarce 43
Łączenie Raspberry Pi z Wyliodrin STUDIO 43
Konfiguracja ręczna 45
Łączenie Raspberry Pi z lokalną wersją Wyliodrin STUDIO 46
Łączenie Raspberry Pi z wersją Wyliodrin STUDIO działającą w przeglądarce 47
Omówienie Wyliodrin STUDIO 50
Wdrażanie aplikacji na Raspberry Pi 52
Podsumowanie 56

Rozdział 3. Inteligentny system cyfrowych ekranów informacyjnych 57

Niezbędne składniki 58
Architektura aplikacji 59
Electron 60
Aplikacja 60
Kod źródłowy 61
Instalacja niezbędnych bibliotek 66
Uruchamianie aplikacji 68
Łączenie z Internetem 70
Aranżowanie interfejsu 76
Podsumowanie 79

Rozdział 4. Inteligentny system dystrybucji wody sodowej 81

Niezbędne składniki 82
Interaktywny dystrybutor wody sodowej 83
Plik main.js 83
Interfejs użytkownika 84
Instalacja wymaganych modułów 92

Budowanie dystrybutora 93
Schemat 93
Aplikacja 94
Instalacja modułów 96
Łączenie systemu z Internetem 97
Konfigurowanie konta Ubidots 97
Inicjowanie wartości widżetu 99
Obliczanie ilości płynu 100
Tworzenie pulpitu 103
Podsumowanie 105

Rozdział 5. Inteligenty system reklamowy 107

Niezbędne składniki 108
Zbieranie informacji z otoczenia 110
Podłączanie modułu kamery 110
Włączanie kamery 112
Kod 112
Personalizacja treści 117
Konfigurowanie konta Microsoft Cognitive Services 118
Przetwarzanie obrazu 120
Personalizacja treści 122
Zdalna aktualizacja obrazów źródłowych 124
Tworzenie konta usługi Google 125
Przekazywanie plików do usługi Google Drive 128
Integracja Google Drive API w aplikacji 129
Podłączanie kamery USB 133
Monitorowanie środowiska 134
Podsumowanie 139

Rozdział 6. Inteligentny system pomiarowy używający serwera przemysłowego 141

Architektura aplikacji przemysłowych 142
Niezbędne składniki 144
Interfejs inteligentnej wtyczki elektrycznej 145
Konfigurowanie inteligentnej wtyczki elektrycznej HS110 przy użyciu aplikacji Kasa 146
Konfigurowanie inteligentnej wtyczki elektrycznej HS110 przy użyciu zestawu SDK języka Python 147
Pisanie sterownika wtyczki zasilania 152
Serwer OPC UA 156
Zmienne OPC UA 159
Serwer OPC UA 160
OPC UA Commander 163
ProSys OPC UA Client 165
Sterownik inteligentnej wtyczki elektrycznej 166
Zapisywanie wartości energii 167
Włączanie i wyłączanie wtyczki elektrycznej 173
Składanie wszystkiego razem 176
Podsumowanie 177

Rozdział 7. Przechowywanie i przetwarzanie danych 179

Niezbędne składniki 180
Używanie bazy danych MariaDB do przechowywania danych 181
Instalacja MariaDB 182
Konfiguracja zewnętrznej pamięci masowej 183
Konfigurowanie modelu danych 192
Uaktualnienie do używania wielu wtyczek inteligentnych 196
Model danych OPC UA 197
Nowy sterownik inteligentnej wtyczki 202
Przechowywanie informacji w bazie danych 215
Podsumowanie 228

Rozdział 8. Wykresy danych 229

Niezbędne składniki 230
Wprowadzenie 230
Instalacja oprogramowania Docker 230
Instalacja oprogramowania Grafana 233
Dodawanie źródła danych MariaDB. 237
Pulpit 239
Podsumowanie. 247

Indeks 249

O autorach

Ioana Culic jest obecnie doktorantką w dziedzinie Internetu rzeczy i współzałożycielką firmy Wyliodrin, która oferuje edukacyjne i przemysłowe rozwiązania IoT. Pracuje jako asystentka na Politechnice w Bukareszcie w Rumunii, a także uczy technologii IoT licealistów i studentów na różnych wydarzeniach już od 5 lat. Pomimo technicznego wykształcenia Ioana zawsze pasjonowała się pisaniem i udało jej się połączyć te zamiłowania. Publikuje artykuły w magazynach, takich jak *MagPi* oraz *Make:*, a także książki o technologiach Internetu rzeczy.

Alexandru Radovici uzyskał doktorat w dziedzinie mobilnych technologii informatycznych i pracuje jako adiunkt na Politechnice w Bukareszcie w Rumunii, ucząc tematów związanych z systemami operacyjnymi, kompilatorami i Internetem rzeczy. Alexandru wierzy w potęgę edukacji, a nauczanie jest jego pasją. Dlatego14 lat temu założył organizację pozarządową, która skupia się na organizowaniu wydarzeń edukacyjnych związanych z IT. Alexandru jest współzałożycielem i CTO firmy Wyliodrin, związanej z najnowszymi technologiami IoT.

Cristian Rusu uzyskał tytuł magistra i doktora na Politechnice w Bukareszcie w Rumunii w latach 2011 i 2012, odpowiednio. Obecnie jest pracownikiem naukowym post-doc we Włoskim Instytucie Technologii (Istituto Italiano di Tecnologia, IIT) w Genui we Włoszech i zajmuje się uczeniem maszynowym i big data, a także ich zastosowaniami w problemach świata rzeczywistego. Jego zainteresowania badawcze obejmują informatykę i przetwarzanie sygnałów z zastosowaniem w komunikacji bezprzewodowej, reprezentacjami rzadkimi, uczeniem słownikowym, uczeniem maszynowym i numerycznej algebrze liniowej. W kontekście komunikacji bezprzewodowej skupia swoje zainteresowania na systemach MIMO, mmWave i komunikacji bezzałogowych statków powietrznych (UAV).

O recenzencie technicznym

Sai Yamanoor jest inżynierem systemów wbudowanych, pracującym w firmie związanej z gazami technicznymi w Buffalo w stanie Nowy Jork. Jego zainteresowania, głęboko zakorzenione w majsterkowaniu (DIY) i sprzęcie open source, obejmują wytwarzanie gadżetów, które pomagają w modyfikacji zachowań. Opublikował dwie książki wraz z bratem, a wolny czas lubi poświęcać na budowanie rzeczy, które poprawiają jakość życia. Portfolio jego projektów można znaleźć pod adresem `http://saiyamanoor.com`.

Wstęp

Podczas paru ostatnich lat Internet rzeczy (IoT) stał się dojrzałą technologią z zastosowaniami na rynkach przemysłowym i konsumenckim. Rewolucja IoT obiecuje utworzyć inteligencję otoczenia, łącząc wszystkie urządzenia i obiekty wokół nas i pozwalając im adaptować się i działać w odpowiedzi na potrzeby ludzkie. Prostym przykładem będzie scenariusz, w którym budzik, wiedząc, że masz spotkanie o 9:00, i uwzględniając warunki drogowe, obudzi Cię o odpowiedniej godzinie bez konieczności konfigurowania poprzedniego wieczora.

Również ekspres do kawy sam przygotuje Ci wtedy kawę, a inne plany dnia będą również brane pod uwagę. Chociaż ten scenariusz nadal jest nieosiągalny, poczyniono już wiele technologicznych udoskonaleń w tym kierunku. Wynikiem jest szeroki zakres wbudowanych urządzeń sprzętowych, różne protokoły komunikacyjne z naciskiem na wydajność i bezpieczeństwo oraz mnóstwo platform oprogramowania wyznaczonych do zarządzania tymi zasobami.

Jedną z najpopularniejszych platform sprzętowych do prototypowania aplikacji IoT jest Raspberry Pi. Hobbiści i studenci na całym świecie integrują to urządzenie w projektach IoT od roku 2012, kiedy została wydana pierwsza wersja. Od kontrolowania oświetlenia domu do automatycznego karmienia zwierząt domowych, urządzenie Pi jest obecne w domach wielu osób. Jednak mało osób uważa Pi za coś więcej niż platformę prototypową lub edukacyjną.

Celem tej książki jest pokazanie nowej perspektywy, jak można wykorzystać Raspberry Pi, integrując to urządzenie w komercyjnych i przemysłowych aplikacjach, które można łatwo skalować i wdrażać jako produkty.

W tej książce przeprowadzimy szereg praktycznych przykładów użycia Raspberry Pi jako rdzenia, wokół którego są budowane w pełni rozwinięte produkty. Mamy nadzieję, że po prześledzeniu wszystkich przykładów zyskacie inne spojrzenie, jak można wykorzystać Raspberry Pi lub inne podobne urządzenia, oraz pełną perspektywę, jak przejść od prototypowania urządzenia domowego od budowania w pełni skalowanego produktu nadającego się do wypuszczenia na rynek.

Dla kogo jest ta książka

Ta książka jest przeznaczona dla pasjonatów budowania systemów Internetu rzeczy: od hobbistów do przedsiębiorców, szczególne tych, którzy chcą rozpocząć biznes w tej dziedzinie. Prezentowane pojęcia są zrozumiałe dla każdego, kto miał pewien kontakt z Raspberry Pi lub podobnym urządzeniem i rozumie podstawowe operacje sterowania stykami. Pewne doświadczenie z programowaniem webowym (HTTP oraz JavaScript/jQuery/Vue.js/Angular.js) jest mile widziane, ponieważ ułatwia szybsze zrozumienie prezentowanych koncepcji.

Jednak projekty są opisane szczegółowo, krok po kroku, więc wystarcza podstawowa znajomość programowania, aby je prześledzić. Ostatecznym celem jest uzyskanie kilku działających prototypów IoT.

Użyte technologie

Struktura rozdziałów zawierających opisy aplikacji wyznacza niezbędne składniki każdego osiągającego sukces systemu IoT: składniki sprzętowe, platformę programistyczną oraz połączenie z innymi urządzeniami i Internetem.

W aspekcie sprzętowym, oprócz opisu, jak zbudować i połączyć składniki z Raspberry Pi, będziemy także prezentować pełen schemat połączeń. Każdy rozdział będzie zaczynać się także od listy składników niezbędnych do zbudowania sprzętu projektu.

W zakresie oprogramowania budowane aplikacje będą składać się z interfejsu użytkownika i logiki aplikacji. Te dwa elementy są programowane przy użyciu technologii HTML i JavaScript. Do sterowania interfejsem użytkownika (UI) wykorzystamy integrację z frameworkiem Vue.js, który pozwala łatwiej i szybciej programować interfejsy użytkownika oparte na języku HTML. Aby uruchamiać te aplikacje na Raspberry Pi, zintegrujemy je z frameworkiem Electron.

Składnik łączności internetowej będzie uwzględniać stosowanie webowych interfejsów API w aplikacjach. W każdym rozdziale będziemy prezentować inną usługę webową (np. interakcję z sieciami społecznościowymi, informacjami o pogodzie lub przetwarzaniem obrazów), która jest żywotnym składnikiem ogólnego systemu i która dostarcza aplikacji szczególny koloryt IoT.

Niezbędny sprzęt

Ta książka ma na celu zaprezentowanie istotnych technologii IoT w bardzo praktyczny sposób. W efekcie każdy rozdział prowadzi Czytelnika przez budowanie prototypu aplikacji IoT wymagającego podłączenia do Raspberry Pi konkretnych składników sprzętowych.

Aby ułatwić przygotowanie do implementacji aplikacji prezentowanych w tej książce, utworzyliśmy listę niezbędnego sprzętu:

- Raspberry Pi
- Monitor HDMI
- Ekran dotykowy
- Przekaźniki 3KY-019 lub podobne
- Trzy pompy wodne
- Zasilacz 5 V
- Moduł kamery Raspberry Pi Camera lub kamera USB
- Czujnik ruchu PIR
- Płytka prototypowa
- Łączówki
- Inteligentna wtyczka elektryczna HS110 firmy TP-Link (najlepiej dwe)
- Raspberry Pi PoE HAT (opcjonalnie)
- Przełącznik sieciowy zgodny z PoE (802.3af) lub iniektor PoE (opcjonalnie)
- Zewnętrzny dysk twardy lub dysk SSD (opcjonalnie, zalecane jest urządzenie USB 3.0)

Kupowanie identycznych składników sprzętowych nie jest konieczne do pomyślnego zaimplementowania aplikacji. Wiele z nich można zastąpić innym, podobnym sprzętem. Dlatego zalecamy, aby przed rozpoczęciem przeprowadzić krótką analizę wymaganego sprzętu i innych dostępnych opcji.

Poruszane tematy

W rozdziale 1 przedstawiamy dziedzinę Internetu rzeczy i podstawową architekturę aplikacji IoT. Prezentujemy główne cechy komercyjnych i przemysłowych systemów IoT, kładąc nacisk na przejście od prototypowania do budowania aplikacji produkcyjnych.

Rozdział 2 zawiera przegląd istniejących środowisk programistycznych do budowania systemów IoT. Prowadzimy Czytelnika przez proces konfiguracji wymagany do połączenia Raspberry Pi z Wyliodrin STUDIO.

W rozdziale 3 wprowadzamy podstawowe koncepcje, takie jak tworzenie opartego na interfejsie użytkownika systemu IoT oraz sposób dołączenia składnika internetowego do aplikacji. Końcowym wynikiem jest webowa platforma IoT, która wyświetla bieżące warunki atmosferyczne.

W rozdziale 4 prowadzimy Czytelnika przez budowanie inteligentnego dozownika wody sodowej przy użyciu HTML oraz Vue.js. Kładziemy także nacisk na znaczenie oraz sposób osiągnięcia zdalnego monitorowania wdrożonych systemów.

W rozdziale 5 skupiamy się na integracji możliwości fotografii i wideo w rozwiązaniach IoT. Prezentujemy moduł kamery Pi Camera oraz sposób sterowania nim, aby móc zbudować inteligentny system reklamowy, który adaptuje reklamy do obecnej widowni.

W rozdziale 6 wprowadzamy technologie przemysłowe, skupiając się na tym, jak używać protokołu OPC UA do sterowania systemami inteligentnego domu, a w naszym przypadku wtyczką elektryczną.

W rozdziale 7 skupiamy się na implementacji przemysłowego protokołu komunikacyjnego OPC UA. W tym przypadku rozszerzamy projekt zaimplementowany w rozdziale 6, aby przy użyciu tego protokołu systematycznie zbierać dane z wielu wtyczek elektrycznych.

W rozdziale 8, ostatnim, wprowadzamy technologie open source do tworzenia wykresów i wizualizacji danych, rozbudowując projekt wytworzony w rozdziale 7.

Rozdział 1

Przegląd systemów IoT

W tym rozdziale podajemy ogólny opis Internetu rzeczy (Internet of Things, IoT), szczególnie skupiając się na aspektach komercyjnych i przemysłowych. Przedstawiamy podstawową terminologię i technologie otaczające IoT, historię i bieżący stan tej techniki, w tym wszystkie główne składniki, urządzenia sprzętowe, wytwarzanie oprogramowania i protokoły komunikacyjne.

Co to jest przemysłowy Internet rzeczy?

Główną ideą stojącą za Internetem rzeczy jest łączenie systemów elektronicznych, które mogą odczuwać środowisko lub oddziaływać z nim i komunikować się ze sobą nawzajem. Chociaż typowe przykłady IoT obejmują codzienne obiekty i zastosowania, założenia IoT mogą być także stosowane w systemach komercyjnych i przemysłowych, prowadząc do lepszych wyników i poprawy wydajności. Zatem niejako w ramach IoT napotykamy szczególne pojęcie przemysłowego Internetu rzeczy (Industrial Internet of Things, IIoT), odnoszące się do produktów komercyjnych i przemysłowych.

Rynki przemysłowe i konsumenckie są ukierunkowane na różne potrzeby i proponują różne rozwiązania i produkty, jednak w przypadku budowania systemu IoT podstawowe cechy i architektury są oparte o zbiór podobnych zasad. Tymi zasadami zajmiemy się w tym rozdziale.

Najpierw wprowadzimy pewne podstawowe definicje IoT i IIoT.

Chociaż nie ma jedynej definicji IoT (patrz, np. „stale zmieniająca się definicja IoT" organizacji IEEE[1]), wybraliśmy, aby zaprezentować następujący opis podany przez organizację Internet Engineering Task Force (IETF) w roku 2010.

> *Podstawowa idea polega na tym, że IoT będzie łączyć obiekty wokół nas (elektroniczne, elektryczne i nieelektryczne), abyt zapewniać płynną komunikację i kontekstowe usługi świadczone przez te obiekty. Rozwój etykiet RFID, czujników, elementów wykonawczych, telefonów komórkowych sprawia, że jest możliwe zmaterializowanie IoT, który będzie prowadził interakcję i wzajemną współpracę, aby sprawiać, że usługa jest lepsza i dostępna w dowolnym czasie i z dowolnego miejsca.*
>
> — Internet Engineering Task Force

Podajemy także opis *rzeczy* w Internecie rzeczy.

> *W wizji IoT „rzeczy" mogą być bardzo różne, takie jak komputery, czujniki, osoby, elementy wykonawcze, lodówki, telewizory, pojazdy, telefony komórkowe, ubrania, żywność, lekarstwa, książki itp. Te rzeczy są klasyfikowane w trzech zakresach: ludzie, maszyny (na przykład czujnik, siłownik itp.) oraz informacje (na przykład ubrania, żywność, lekarstwa, książki itp.). Te „rzeczy" powinny być identyfikowane przynajmniej w jeden unikatowy sposób, umożliwiający adresowanie i wzajemną komunikację oraz weryfikowanie ich tożsamości. Tutaj, jeśli „rzecz" jest zidentyfikowana, nazywamy ją „obiektem".*
>
> — Internet Engineering Task Force

Natomiast, aby zdefiniować IIoT, wybraliśmy opis firmy HP[2].

> *IIoT składa się z maszyn połączonych internetowo oraz zaawansowanych platform analitycznych, które przetwarzają wytwarzane przez nie dane. Urządzenia IIoT mają zakres od małych czujników środowiskowych do złożonych robotów przemysłowych. Chociaż słowo „przemysłowy" może przywoływać na myśl magazyny, stocznie*

1 https://iot.ieee.org/definition.html
2 www.hpe.com/emea_europe/en/what-is/industrial-iot.html

i fabryki, technologie IIoT obejmują wiele różnorodnych, obiecujących branż, w tym rolnictwo, opiekę zdrowotną, usługi finansowe, sprzedaż detaliczną i reklamy.

Przemysłowy Internet rzeczy jest podkategorią Internetu rzeczy, który także obejmuje aplikacje ukierunkowane na klienta, takie jak urządzenia, które można na siebie założyć, technologię inteligentnych domów oraz samochody autonomiczne. Urządzenia z wbudowanymi czujnikami, maszyny i infrastruktura, które transmitują dane przez Internet i są zarządzane programowo, charakteryzują obie te koncepcje.

— HP

Cechy IoT

Znając te podstawowe definicje, omówimy teraz pewne podstawowe cechy IoT. W systemie IoT wyróżniamy *rzeczy* stanowiące jego podstawę. Dowolne rozwiązanie IoT ma na celu wniesienie inteligencji do już istniejących obiektów/urządzeń i sprawienia, aby działały autonomicznie. *Inteligencja* takiego rozwiązania jest oparta na odczuwaniu i akcji, łączności, gromadzeniu dużych ilości danych oraz możliwościach przetwarzania i przechowywania, skutkujących następującymi istotnymi cechami systemu IoT:

- **Łączność –** to jest podstawa dowolnego rozwiązania IoT; czujniki są połączone ze sobą i z urządzeniami, urządzenia są połączone ze sobą i z Internetem, na poziomie lokalnym lub globalnym, a możliwość wymiany danych jest siłą napędową IoT.
- **Zarządzanie rzeczami –** celem dowolnego urządzenia IoT jest odczuwanie i interakcja ze środowiskiem, a to może być realizowane tylko przez obiekty fizyczne, które w ogólności nazywamy rzeczami.
- **Heterogeniczność –** ekosystem IoT jest zbudowany na podstawie różnorodnych urządzeń sprzętowych, infrastruktur sieciowych oraz platform przetwarzania, które są potrzebne do wymiany informacji i działania, aby osiągnąć wspólny cel.
- **Gromadzenie danych –** inteligencja systemów IoT jest oparta na danych zbieranych przez czujniki, te dane są przetwarzane, a następnie konwertowane do użytecznych informacji.
- **Dynamika –** infrastruktury IoT zmieniają się stale, sieci dynamicznie dostosowują parametry, czujniki mogą się podłączać i rozłączać, urządzenia mogą wchodzić

w tryb bezczynności, czuwania lub uśpienia, a systemy powinny utrzymywać poprawne działanie, niezależnie od zmian występujących w środowisku.

- **Duża skala –** w roku 2020 liczba urządzeń połączonych z Internetem w przybliżeniu dochodzi do 20 miliardów[3] i rośnie w tempie wykładniczym, a to wymaga infrastruktury i platform zdolnych do zarządzania tak wielkimi liczbami połączeń.
- **Autonomia –** wiele spośród urządzeń inteligentnych z założenia ma być wdrażanych w odległych miejscach, a zatem urządzenia te muszą podejmować decyzje bez interwencji ludzkiej, a jednocześnie mogą nie mieć dostępu do stałego źródła zasilania, zależąc od baterii lub alternatywnych źródeł energii. W takich warunkach urządzenia wymagają również zdalnego monitorowania, sterowania, a nawet aktualizacji lub naprawy.
- **Prywatność i bezpieczeństwo –** oto kwestie wymagające najwyższej troski, jeśli chodzi o IoT. Podłączenie systemów ogrzewania lub urządzeń medycznych do Internetu naraża je na znaczne ryzyko, a kompromitacja lub wrogie przejęcie sterowania takim systemem może mieć katastrofalne skutki. Równie ważne jest, aby użytkownicy systemów IoT przez cały czas wiedzieli, jakie dane są gromadzone (oraz zgadzali się na to).

Rozważmy system IoT inteligentnego budynku, który monitoruje temperaturę wewnątrz budynku i ma dostęp do kalendarzy mieszkańców. Na podstawie tych danych może zapewnić, że kiedy mieszkańcy wracają do domu lub już w nim są, ustawiana jest preferowana przez nich temperatura otoczenia, a gdy są poza domem, systemy ogrzewania i chłodzenia są optymalizowane, aby zredukować zużycie energii i koszt. Taki system wymaga połączenia czujników temperatury z systemami HVAC (ogrzewania, wentylacji i klimatyzacji), a także pobierania danych lokalizacji mieszkańców. Ponadto, aby ten system był skuteczny, wymaga autonomicznego i nieprzerwanego działania, aby zapewnić, że dane dotyczące zachowania użytkowników są bezpiecznie przechowywane i używane. Ponieważ informacje o lokalizacji mieszkańców muszą być dostępne dla systemu, kwestie prywatności i zabezpieczeń są pierwszoplanowe. Na przykład nieautoryzowany dostęp do tych informacji może dokładnie poinformować złodziei, kiedy

3 www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent- rom-2016

dom jest pusty. Na tym prostym przykładzie możemy szybko rozpoznać wiele z wcześniej wspomnianych cech.

Wymaganiem niezbędnym do sukcesu IoT jest to, że ludzie potrzebują wygody i bezpieczeństwa, kiedy korzystają z nowych technologii. Niestety technologie IoT wprowadziły także nowe szczególne kwestie dotyczące zabezpieczeń i związane z tym zagrożenia. Jeśli wszystkie urządzenia, które nas otaczają byłyby połączone z Internetem, wtedy naruszenie zabezpieczeń mogłoby skutkować zniszczeniami w świecie rzeczywistym, obejmującymi zarówno dobytek, jak i ludzi. Jednym z najgorszych zagrożeń zabezpieczeń IoT jest użycie *botnetów*. Botnet to zbiór urządzeń, których bezpieczeństwo zostało skompromitowane i są używane przez inną osobę, która kontroluje ich w celu dokonania cyberataków względem konkretnego celu. Zwykle te ataki przyjmują formę Distributed Denial-of-Service (DDoS). Internet rzeczy jest szczególnie podatny na taki atak, ponieważ duża liczba urządzeń jest podłączona z sieciami IoT. Dwa ostatnie sławne ataki zdarzyły się w roku 2016 i były związane z botnetami Mirai[4] oraz Remaiten[5].

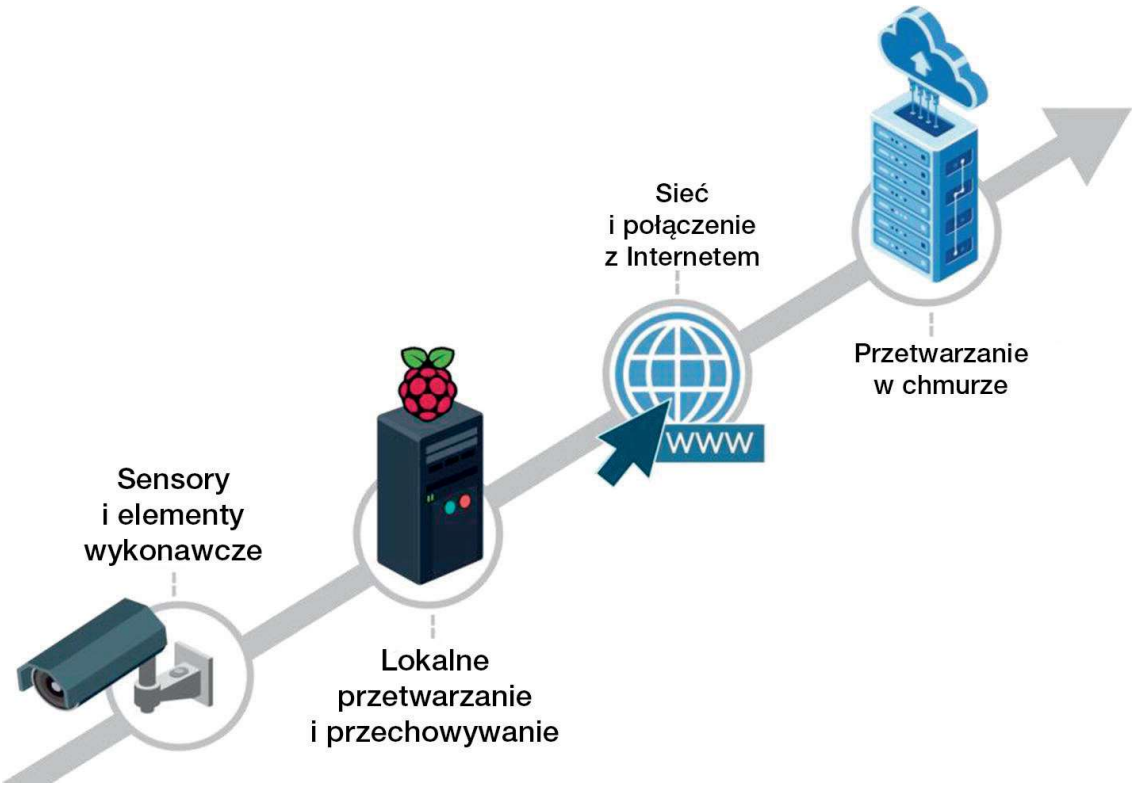
Architektura IoT

W ogólności rozwiązanie IoT działa następująco: wykrywa warunki środowiska za pomocą czujników, analizuje zebrane dane i reaguje na podstawie wniosków. Aby lepiej zilustrować składniki ogólnego systemu IoT i sposób, w jaki przeprowadza wzajemne interakcje, specjaliści wprowadzili stos IoT. Ponieważ nadal brakuje gruntownej standaryzacji IoT, istnieją różne wersje stosu, bardziej lub mniej szczegółowe, skupiające się na różnych aspektach. Niemniej jednak, z szerokiej perspektywy, większość z nich składa się z następujących składników:

- Czujniki i elementy wykonawcze
- Lokalne przetwarzanie i przechowywanie
- Połączenie sieciowe i internetowe
- Przetwarzanie w chmurze

4 https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/

5 www.securityweek.com/new-remaiten-malware-builds-botnet-linux-based-routers



Rysunek 1-1. *Stos Internetu rzeczy*

Na podstawie rysunku 1-1 widać, że *czujniki i elementy wykonawcze* są umieszczone na dole stosu, ponieważ są elementami komunikującymi się bezpośrednio ze środowiskiem. W górę stosu umieściliśmy urządzenia do lokalnego przetwarzania i przechowywania, nazywane także *urządzeniami brzegowymi*. Są to komputery, takie jak Raspberry Pi, które mają możliwość wymiany informacji z urządzeniami peryferyjnymi i mają minimalne możliwości obliczeniowe, więc mogę wstępnie przetwarzać dane otrzymywane z czujników. Na wyższym poziomie urządzenia brzegowe mogę być połączone z urządzeniami sieciowymi, takimi jak routery, i mieć dostęp do *Internetu*. W końcu na górze stosu jest *chmura*, gdzie duże ilości danych pochodzących z wielu urządzeń brzegowych są przechowywane, a z pomocą uczenia maszynowego i sztucznej inteligencji (artificial intelligence, AI), mogą być używane do podejmowania ważnych decyzji i wykonywania złożonych analiz lub predykcji przyszłych zachowań systemów i osób.

Systemy IIoT

Wiele branż spodziewa się największych korzyści z IoT. W tym przypadku mamy do czynienia m.in. z produkcją i liniami montażowymi, szybami naftowymi, elektrowniami słonecznymi, wiatrakami. Chociaż te systemy mają wyraźnie zdefiniowany cel i działanie, producenci stale poszukują sposobów zwiększenia ich wydajności i redukcji kosztów operacyjnych. Dlatego perspektywa systemów, które mogą samodzielnie analizować, adaptować i optymalizować na podstawie środowiska lub innych parametrów, jest interesująca dla większości firm przemysłowych.

Do tej pory zbadaliśmy ogólne cechy i architektury systemów IoT. Chociaż dotyczą one także platform IIoT, istotne jest zrozumienie, że systemy przemysłowe mają szczególne cechy, z którymi trzeba się liczyć:

- **Warunki środowiskowe –** to jedna z głównych przyczyn budowania autonomicznych maszyn przemysłowych, ponieważ w wielu przypadkach warunki pracy w fabrykach nie są sprzyjające dla ludzi, którzy mogą być narażeni na oddziaływanie substancji chemicznych, wysokich temperatur lub wysokiej wilgotności, prowadzące do długoterminowych problemów zdrowotnych.
- **Koszty –** wszystkie firmy mają na celu możliwie najlepszą wydajność ekonomiczną, a zatem koszty operacyjne są ważnym czynnikiem decyzyjnym podczas wprowadzania nowych systemów lub urządzeń do produkcji lub linii montażowych.
- **Czas przestoju –** czynności odbywające się w elektrowniach są zwykle nieprzerwane, poza konkretnymi, ograniczonymi okresami wykonywania konserwacji. Oczywiście są wyjątki, ponieważ systemy mogą ulegać awarii, ale wtedy czas przestoju przekłada się poważne straty finansowe.

Na podstawie tych cech, dowolne rozwiązanie IoT implementowane w przemyśle musi spełniać następujące wymagania:

- **Solidność –** dowolny produkt przemysłowy musi być dostosowany do środowiska, w którym zostanie wdrożony. Powinien wytrzymać surowe warunki pracy i właśnie dlatego większość urządzeń przeznaczonych do użycia w przemyśle jest *wzmacniana*.

- **Stabilność –** urządzenie działające nietypowo lub nieoczekiwanie ulegające awarii skutkuje czasami przestoju. Większość urządzeń przemysłowych ma wymaganie ciągłej pracy (czasami zbliżonej do technicznych ograniczeń) przez potencjalnie długie okresy.
- **Czas rzeczywisty –** niektóre maszyny wdrażane w fabrykach wymagają bardzo szybkich reakcji na wyzwalacze lub zdarzenia w środowisku. Czasy reakcji są istotne, aby zapewnić dokładne odczyty i wyniki oraz ogólną synchronizację zasobów systemowych.

Ankieta przeprowadzona w roku 2015 przez bank Morgan Stanley i czasopismo *Automation World* nakreśliła, że główną zachętą do przyjęcia przemysłowego Internetu rzeczy (IIoT) jest żądanie poprawienia wydajności operacyjnej, a następnie żądanie poprawy produktywności[6].

Jednym z pierwszych kroków w kierunku zwiększenia wydajności i produktywności procesu jest analiza jego bieżącego stanu i znalezienie sposobów poprawy. Ta potrzeba wyjaśnia szerokie przyjęcie technologii IoT na rynku przemysłowym. Główną cechą systemów IoT jest to, że używają czujników do zbierania informacji o środowisku, sprawiając, że są odpowiednie do pomocy w zwiększeniu produktywności i redukcji kosztów. Poza aspektem big data i analitycznym Internetu rzeczy, regularne monitorowanie sprzętu przemysłowego przy użyciu czujników może zapewniać bardziej dokładne dane w porównaniu z pomiarami prowadzonymi przez ludzi. Celem jest umożliwienie wczesnego wykrywania psucia się maszyny i łatwiejsze zapobieganie nieoczekiwanym awariom, prowadzące do redukcji koszu związanego z konserwacją i czasem przestojów.

Historyczna potrzeba zwiększenia wydajności operacyjnej procesów przemysłowych prowadziła do wynalezienia wielu rozwiązań monitorowania i sterowania, poprzedników dzisiejszych platform IIoT.

System SCADA

IIoT nie jest historycznie pierwszym podejściem do poprawy i modernizacji infrastruktury przemysłowej.

6 www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/

SCADA (Supervisory Control and Data Acquisition) to przemysłowy system sterowania wynaleziony w latach 50. XX w. Ten system został zaprojektowany w celu integracji z infrastrukturami fabryk i umożliwia monitorowania i sterowania operacjami przemysłowymi. System SCADA był używany powszechnie w takich dziedzinach przemysłu, jak energetyka, produkcja, wydobywanie i przetwarzanie ropy i gazu, transport, zarządzanie odpadami, przemysł spożywczy i wielu innych. Obecnie systemy SCADA są nadal szeroko używane do zarządzania przepływem ruchu drogowego i regulowania sygnalizacji świetlnej.

W miarę upływu czasu systemy SCADA były stale poprawiane w czterech generacjach technologicznych: początkowa struktura monolityczna, fazy rozproszone i połączone siecią, a w końcu ich ewolucja do nowoczesnych systemów IIoT[7].

Systemy SCADA używają czujników, które pobierają dane, takie jak temperatura, wilgotność lub wibracja, dotyczące maszyn przemysłowych i wyświetlają je w interfejsie użytkownika z zastosowaniem wykresów i innych elementów wizualnych. Z drugiej strony system jest także połączony z zaworami, silnikami, pompami i innymi mechanizmami sterującymi, które mogą być zarządzane z tego samego interfejsu użytkownika bez potrzeby bezpośredniego oddziaływania człowieka na maszynę przemysłową. Ponadto pracownicy fabryki mogą projektować procedury, aby system reagował automatycznie na zmiany w środowisku. Na przykład możemy zaprogramować maszynę, aby się wyłączała, jeśli pewne parametry systemu (np. temperatura) osiągną pewien poziom uważany za krytyczny.

System SCADA można także wdrażać w dużych połączonych systemach przemysłowych, co prowadzi do pytania: *czym SCADA różni się od nowoczesnych rozwiązań przemysłowego Internetu rzeczy?*

Chociaż system SCADA wnosi scentralizowane monitorowanie i sterowania do platformą przemysłowych, brakuje mu inteligencji, która jest szczególna dla systemów IoT; a dokładniej brakuje mu składnika chmurowego stosu IoT. To z kolei ogranicza system do podejmowania prostych lokalnych decyzji. Co gorsze, historycznie te decyzje były podejmowane przez ludzkich operatorów, wprowadzając możliwość pomyłek. Z tego powodu wielu producentów przemysłowych platform IoT zdecydowało się rozszerzyć

7 www.engineersgarage.com/articles/scada-systems

infrastrukturę SCADA i wnieść możliwości uczenia maszynowego i sztucznej inteligencji oraz usunąć ludzkie działania z pętli.

Ponieważ dwa znaczące wypadki katastrof w XX wieku w elektrowniach Three Mile Island i Czernobyl także obejmowały błędy operatów ludzkich, mamy nadzieję, że możliwości sztucznej inteligencji będą w stanie wyeliminować lub przynajmniej znacznie zredukować przyszłe zagrożenia takimi destrukcyjnymi zdarzeniami.

Ponadto jedną z najistotniejszych wad systemu SCADA jest bezpieczeństwo, a dokładniej jego brak. Ponieważ ten system był zaprojektowany, kiedy platformy nie były połączone z żadnym zewnętrznym systemem, występowanie naruszenia zabezpieczeń było mało prawdopodobne. Obecnie SCADA polega na mechanizmie zabezpieczeń przez niejawność (tajność projektu i implementacji), ale ostatnie odkrycia luk, takich jak Spectre i Meltdown, dowiodły, że jest to nieskuteczne. Niechlubnym przykładem niedawnego naruszenia zabezpieczeń jest atak w roku 2010 o nazwie Stuxnet na irańskie obiekty przemysłowe, gdzie atakujący byli w stanie zalogować się do bazy danych SCADA i ukraść pliki projektowe i sterujące[8]. Nowszym i mniej spektakularnym, ale równie ważnym przykładem jest włamanie hakerskie do systemów ruchu drogowego w dużych miastach[9].

Od prototypowania do systemów przemysłowych

Pierwszym krokiem podczas budowania produktu IoT jest sporządzenie prototypu, a tutaj skorzystamy z popularności IoT wśród społeczności inżynierów, majsterkowiczów i hobbystów. Istnieje mnóstwo książek i czasopism o IoT, a także wydarzeń dedykowanych społeczności majsterkowiczów (do-it-yourself, DIY), a proste wyszukiwanie online prowadzi do tysięcy samouczków, jak zbudować połączony system oświetlenia lub sprawić, że odkurzacz będzie inteligentny. Jednak, gdy prototyp już działa, występuje kilka dodatkowych aspektów, z którymi trzeba się liczyć, zanim urządzenie będzie mogło rzeczywiście zostać sprzedane, a następnie wdrożone w środowisku przemysłowym:

- **Stabilność –** ważne jest, aby zapewnić, że system działa bez nieoczekiwanych zakłóceń, a jeśli błąd wystąpi, urządzenie jest w stanie wrócić do działania bez

8 http://archive.is/20120525053210/http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

9 https://resources.infosecinstitute.com/hacking-traffic-light-systems