

Computer Communications and Networks

Zaigham Mahmood *Editor*

# The Internet of Things in the Industrial Sector

Security and Device Connectivity, Smart  
Environments, and Industry 4.0

 Springer


# Computer Communications and Networks

## Series Editors

Jacek Rak, Department of Computer Communications, Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Gdansk, Poland

A. J. Sammes, Cyber Security Centre, Faculty of Technology, De Montfort University, Leicester, UK

## Editorial Board

Burak Kantarci , School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada

Eiji Oki, Graduate School of Informatics, Kyoto University, Kyoto, Japan

Adrian Popescu, Department of Computer Science and Engineering, Blekinge Institute of Technology, Karlskrona, Sweden

Gangxiang Shen, School of Electronic and Information Engineering, Soochow University, Suzhou, China

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers, and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

More information about this series at <http://www.springer.com/series/4198>

Zaigham Mahmood  
Editor

# The Internet of Things in the Industrial Sector

Security and Device Connectivity, Smart  
Environments, and Industry 4.0

 Springer

*Editor*

Zaigham Mahmood  
Northampton University  
Northampton, UK

Shijiazhuang Tiedao University  
Shijiazhuang, Hebei, China

ISSN 1617-7975                      ISSN 2197-8433 (electronic)  
Computer Communications and Networks  
ISBN 978-3-030-24891-8              ISBN 978-3-030-24892-5 (eBook)  
<https://doi.org/10.1007/978-3-030-24892-5>

© Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*To:  
Imran, Zoya, Arif, Hanya and Ozair  
For their Love and Support*

# Preface

## Overview

The Internet of Things, abbreviated as IoT, is the extension of Internet connectivity into self-configuring sensor-enabled smart objects. It is a vision of pervasive computing where smart devices connect to each other in a seamless manner, to establish a unified physical-virtual world. The attraction of the IoT is such that the wave of connectivity is now moving beyond laptops and smartphones, to building autonomous cars, developing smart cities, designing intelligent wearables, and providing connected healthcare. According to Gartner, by 2020, connected devices across all technologies will reach at least 20 billion.

In the industrial sector, the IoT is promising to reshape the entire landscape as its business value has been recognized to be profound. It is for this reason that Internet of Things in the industrial sector, also called the Industrial Internet, often referred to as Industrial IoT (IIoT), is becoming increasingly more pervasive, especially as digitisation and automation are becoming a business reality for many organisations in sectors such as manufacturing, logistics, oil and gas, water and power, renewable energy, mining, transportation, aviation and many more. Thus, market opportunities for the IIoT paradigm are huge. According to one research, the IIoT market is estimated to reach \$125 Billion by 2021. The driving philosophy behind IIoT is that smart machines are better than humans at accurately capturing, transmitting and processing of real-time data for the extraction of business intelligence and corporate decision-making.

The underlying technologies include distributed computing, cloud paradigm, ambient intelligence, machine learning, artificial intelligence and machine-to-machine communication. A typical IIoT system consists of intelligent systems (applications, controllers, sensors and security mechanisms), data communication infrastructures (cloud computing, edge computing, etc.), data analytics (to support business intelligence and corporate decision-making) and most importantly the human element.

The IIoT vision holds great potential for nearly all aspects of industrial operations including quality control, predictive maintenance, real-time asset health monitoring, sustainability and business continuity. The IIoT also promises enhanced safety, better reliability, smart metering, as well as efficient inventory management, equipment tracking and facilities management. According to IBM, the latent business value that can be unlocked by the Industrial IoT vision could be as much as \$3.7 trillion in 2025. However, there are also numerous challenges to the adoption of IIoT including operational complexity, connectivity challenges, service availability, data security, diversity of connected objects, lack of ubiquitous interoperability, high cost of required infrastructure, complexity of big data analytics, as well as insufficiency of Internet bandwidth and unreliable nature of the present-day Internet.

It is in the above context that this book is set. The focus of the volume is on the use of IoT in the industrial environment, in particular the relevant principles, frameworks, architectures, technologies and applications, as well as practical suggestions and solutions to the inherent barriers and challenges. In this book, thirty-seven researchers and practitioners of international repute have presented latest research, current trends and case studies, as well as suggestions for further understanding, development and enhancement of the much attractive Industrial IoT vision.

## **Objectives**

The aim of this volume is to present and discuss the IoT vision as extended to the industrial environment. The general objectives include the following:

- To provide the latest research and practice with respect to frameworks, mechanisms, benefits and limitation relating to IIoT
- To present case studies describing challenges, best practices and solutions with respect to IoT environments in industrial settings
- To develop a textbook and complete reference for students, researchers and practitioners in the subject area of distributed computing and IoT

## **Organization**

There are 13 chapters in this book. These are organized into four parts, as follows:

### **Part I Concepts, Processes and Limitations**

This part of the book has a focus on concepts and technologies relating to the Industrial IoT vision. There are three chapters in this part. The first contribution presents a review of the current technologies, development frameworks and



platforms relevant to the IIoT paradigm. The second chapter aims to discuss the underlying principles and industrial processes, illustrating various case studies relating to industries in Japan. The next chapter considers three R&D projects based in the IIoT domain and explores inherent challenges with reference to requirements elicitation and design of projects.

## **Part II Frameworks and Methodologies**

This part of the book also comprises three chapters. The focus is on methods and mechanisms. The first contribution introduces the notion of Internet of measurement things and presents an architectural framework for IoT applications in the calibration industry. The second chapter discusses the modelling of industrial IoT systems, in particular the architecture of a smart traffic system, using data distribution service mechanism. The third presentation looks at the constraints and minimum requirements based on the notion of Automated Pyramid to develop an optimum IIoT system.

## **Part III Connectivity and Novel Technologies**

This part looks at the connectivity aspects of the IoT. It comprises three chapters. The first chapter presents blockchain mechanisms to resolve security vulnerabilities that often exist in IoT-based systems. The second contribution introduces the application of visible light communication in the IoT/IIoT context and investigates the promised benefits and inherent limitations. The third contribution in this part explores the use of low-power long-range WAN technologies, especially for the IoT vision, and presents results of an experiment conducted at a Brazilian University.

## **Part IV Applications and Use Case Scenarios**

This part, comprising four chapters, has a focus on IIoT applications. The first two contributions present discussions on the implementation of IIoT vision for the renewable energy and healthcare sectors. Emphasis is, in one case, on smart microgrids' technology, and in the latter case, on the challenges due to IIoT technologies and on future developments. The third chapter examines real-life examples from the industry that have successfully benefited from IIoT solutions. The final chapter explores the challenges of deploying IIoT vision in Egypt and discusses the inherent challenges and necessary technology trade-offs.

## **Target Audiences**

This current volume is a reference text aimed at supporting a number of potential audiences, including the following:

- *Network Specialists, Hardware Engineers and Security Experts* who wish to adopt the newer approaches to device connectivity, network security, data privacy and sensor-based devices design relevant to the IIoT vision.
- *Students, Academics, Researchers and Practitioners* who have an interest in further enhancing the knowledge of technologies, mechanisms and practices relevant to industrial IoT from a distributed computing perspective.

Northampton, UK/Shijiazhuang, China

Zaigham Mahmood

# Acknowledgements

The editor acknowledges the help and support of the following colleagues during the review, development and editing phases of this text:

- Prof. Zhengxu Zhao, Shijiazhuang Tiedao University, Hebei, China
- Dr. Alfredo Cuzzocrea, University of Trieste, Trieste, Italy
- Dr. Emre Erturk, Eastern Institute of Technology, New Zealand
- Prof. Jing He, Kennesaw State University, Kennesaw, GA, USA
- Josip Lorincz, FESB-Split, University of Split, Croatia
- Aleksandar Milić, University of Belgrade, Serbia
- Prof. Sulata Mitra, Indian Institute of Engineering Science and Technology, Shibpur, India
- Dr. S. Parthasarathy, Thiagarajar College of Engineering, Tamil Nadu, India
- Daniel Pop, Institute e-Austria Timisoara, West University of Timisoara, Romania
- Dr. Pethuru Raj, IBM Cloud Centre of Excellence, Bangalore, India
- Dr. Muthu Ramachandran, Leeds Beckett University, Leeds, UK
- Dr. Lucio Agostinho Rocha, State University of Campinas, Brazil
- Dr. Saqib Saeed, University of Dammam, Saudi Arabia
- Prof. Claudio Sartori, University of Bologna, Bologna, Italy
- Dr. Mahmood Shah, University of Central Lancashire, Preston, UK
- Dr. Fareeha Zafar, GC University, Lahore, Pakistan

I would also like to thank the contributors of this book: 37 authors and co-authors, from academia as well as industry from around the world, who collectively submitted 13 well-researched chapters. Without their efforts in developing quality contributions, conforming to the guidelines and meeting often the strict deadlines, this text would not have been possible.

Grateful thanks are also due to the members of my family—Rehana, Zoya, Imran, Hanya, Arif and Ozair—for their continued support and encouragement. Every good wish, also, for the youngest in our family: Eyaad Imran Rashid Khan and Zayb-un-Nisa Khan.

Northampton, UK/Shijiazhuang, China  
May 2019

Zaigham Mahmood

# **Other Books by Zaigham Mahmood**

## **Security, Privacy and Trust in the IoT Environment**

This reference text has a focus on security and privacy in the Internet of things environments. It also discusses the aspects of user trust with respect to device connectivity. Main topics covered include principles, underlying technologies, security issues, mechanisms for trust and authentication as well as success indicators, performance metrics and future directions. ISBN: 978-3-030-18074-4.

## **Guide to Ambient Intelligence in the IoT Environment: Principles, Technologies and Applications**

This reference text discusses the AmI element of the IoT paradigm and reviews the current developments, underlying technologies and case scenarios relating to AmI-based IoT environments. The book presents cutting-edge research, frameworks and methodologies on device connectivity, communication protocols and other aspects relating to the AmI-IoT vision. ISBN: 978-3-030-04172-4.

## **Fog Computing: Concepts, Frameworks and Technologies**

This reference text describes the state of the art of fog and edge computing with a particular focus on development approaches, architectural mechanisms, related technologies and measurement metrics for building smart adaptable environments. The coverage also includes topics such as device connectivity, security, interoperability and communication methods. ISBN: 978-3-319-94889-8.

## **Smart Cities: Development and Governance Frameworks**

This text/reference investigates the state of the art in approaches to building, monitoring, managing and governing smart city environments. A particular focus is placed on the distributed computing environments within the infrastructure of smart cities and smarter living, including issues of device connectivity, communication, security and interoperability. ISBN: 978-3-319-76668-3.

## **Data Science and Big Data Computing: Frameworks and Methodologies**

This reference text has a focus on data science and provides practical guidance on big data analytics. Expert perspectives are provided by an authoritative collection of 36 researchers and practitioners, discussing latest developments and emerging trends; presenting frameworks and innovative methodologies; and suggesting best practices for efficient and effective data analytics. ISBN: 978-3-319-31859-2.

## **Connected Environments for the IoT: Challenges and Solutions**

This comprehensive reference presents a broad-ranging overview of device connectivity in distributed computing environments, supporting the vision of IoT. Expert perspectives are provided, covering issues of communication, security, privacy, interoperability, networking, access control and authentication. Corporate analysis is also offered via several case studies. ISBN: 978-3-319-70101-1.

## **Connectivity Frameworks for Smart Devices: The Internet of Things from a Distributed Computing Perspective**

This is an authoritative reference that focuses on the latest developments on the Internet of things. It presents state of the art on the current advances in the connectivity of diverse devices and focuses on the communication, security, privacy, access control and authentication aspects of the device connectivity in distributed environments. ISBN: 978-3-319-33122-5.

## **Cloud Computing: Methods and Practical Approaches**

The benefits associated with cloud computing are enormous, yet the dynamic, virtualized and multi-tenant nature of the cloud environment presents many challenges. To help tackle these, this volume provides illuminating viewpoints and case studies to present current research and best practices on approaches and technologies for the emerging cloud paradigm. ISBN: 978-1-4471-5106-7.

## **Cloud Computing: Challenges, Limitations and R&D Solutions**

This reference text reviews the challenging issues that present barriers to greater implementation of the cloud computing paradigm, together with the latest research into developing potential solutions. This book presents case studies, and analysis of the implications of the cloud paradigm, from a diverse selection of researchers and practitioners of international repute. ISBN: 978-3-319-10529-1.

## **Continued Rise of the Cloud: Advances and Trends in Cloud Computing**

This reference volume presents latest research and trends in cloud-related technologies, infrastructure and architecture. Contributed by expert researchers and practitioners in the field, this book presents discussions on current advances and practical approaches including guidance and case studies on the provision of cloud-based services and frameworks. ISBN: 978-1-4471-6451-7.

## **Software Engineering Frameworks for the Cloud Computing Paradigm**

This is an authoritative reference that presents the latest research on software development approaches suitable for distributed computing environments. Contributed by researchers and practitioners of international repute, the book offers practical guidance on enterprise-wide software deployment in the cloud environment. Case studies are also presented. ISBN: 978-1-4471-5030-5.

## **Cloud Computing for Enterprise Architectures**

This reference text, aimed at system architects and business managers, examines the cloud paradigm from the perspective of enterprise architectures. It introduces fundamental concepts, discusses principles and explores frameworks for the adoption of cloud computing. The book explores the inherent challenges and presents future directions for further research. ISBN: 978-1-4471-2235-7.

## **Cloud Computing: Concepts, Technology and Architecture**

This is a textbook (in English but also translated in Chinese and Korean) highly recommended for adoption for university-level courses in distributed computing. It offers a detailed explanation of cloud computing concepts, architectures, frameworks, models, mechanisms, and technologies—highly suitable for both newcomers and experts. ISBN: 978-0-13-338752-0.

## **Software Project Management for Distributed Computing: Life-Cycle Methods for Developing Scalable and Reliable Tools**

This unique volume explores cutting-edge management approaches to developing complex software that is efficient, scalable, sustainable and suitable for distributed environments. Emphasis is on the use of the latest software technologies and frameworks for life-cycle methods, including design, implementation and testing stages of software development. ISBN: 978-3-319-54324-6.

## **Requirements Engineering for Service and Cloud Computing**

This text aims to present and discuss the state of the art in terms of methodologies, trends and future directions for requirements' engineering for the service and cloud computing paradigm. Majority of the contributions in the book focus on requirements' elicitation; requirements' specifications; requirements' classification and requirements' validation and evaluation. ISBN: 978-3-319-51309-6.



## **User-centric E-Government: Challenges and Opportunities**

This text presents a citizen-focused approach to the development and implementation of electronic government. The focus is twofold: discussion on challenges of service availability, e-service operability on diverse smart devices as well as on opportunities for the provision of open, responsive and transparent functioning of world governments. ISBN: 978-3-319-59441-5.

## **Cloud Computing Technologies for Connected Government**

This text reports the latest research on electronic government for enhancing the transparency of public institutions. It covers a broad scope of topics including citizen empowerment, collaborative public services, communication through social media, cost benefits of the cloud paradigm, electronic voting systems, identity management and legal issues. ISBN: 978-1-4666-8629-8.

## **Human Factors in Software Development and Design**

This reference text brings together high-quality research on the influence and impact of ordinary people on the software industry. With the goal of improving the quality and usability of computer technologies, topics include global software development, multi-agent systems, public administration platforms, socio-economic factors and user-centric design. ISBN: 978-1-4666-6485-2.

## **IT in the Public Sphere: Applications in Administration, Government, Politics and Planning**

This reference text evaluates current research and best practices in the adoption of e-government technologies in developed and developing countries, enabling governments to keep in touch with citizens and corporations in modern societies. Topics covered include citizen participation, digital technologies, globalization, strategic management and urban development. ISBN: 978-1-4666-4719-0.

## **Emerging Mobile and Web 2.0 Technologies for Connected E-Government**

This reference highlights the emerging mobile and communication technologies, including social media, deployed by governments for use by citizens. It presents a reference source for researchers, practitioners, students and managers interested in the application of recent technological innovations to develop an open, transparent and more effective e-Government environment. ISBN: 978-1-4666-6082-3.

## **E-Government Implementation and Practice in Developing Countries**

This volume presents research on current undertakings by developing countries towards the design, development and implementation of e-Government policies. It proposes frameworks and strategies for the benefits of project managers, government officials, researchers and practitioners involved in the development and implementation of e-Government planning. ISBN: 978-1-4666-4090-0.

## **Developing E-Government Projects: Frameworks and Methodologies**

This text presents frameworks and methodologies for strategies for the design, implementation of e-Government projects. It illustrates the best practices for successful adoption of e-Government and thus becomes essential for policy makers, practitioners and researchers for the successful deployment of e-Government planning and projects. ISBN: 978-1-4666-4245-4.

# Contents

## Part I Concepts, Processes and Limitations

<b>1 A Review of IoT Technologies, Standards, Tools, Frameworks and Platforms</b> .....	3
Eldar Sultanow and Alina Chircu	
<b>2 Industrial Internet of Things (IIoT): Principles, Processes and Protocols</b> .....	35
Somayya Madakam and Takahiro Uchiya	
<b>3 Systems Development for the Industrial IoT: Challenges from Industry R&amp;D Projects</b> .....	55
Nuno Santos, Francisco Morais, Helena Rodrigues and Ricardo J. Machado	

## Part II Frameworks and Methodologies

<b>4 Internet of Measurement Things: Toward an Architectural Framework for the Calibration Industry</b> .....	81
Mahdi Saeedi Nikoo, M. Cagri Kaya, Michael L. Schwartz and Halit Oguztuzun	
<b>5 Architecture Modeling of Industrial IoT Systems Using Data Distribution Service UML Profile</b> .....	103
Bedir Tekinerdogan, Turgay Çelik and Ömer Köksal	
<b>6 Industrial IoT Projects Based on Automation Pyramid: Constraints and Minimum Requirements</b> .....	121
J. A. López-Leyva, A. Talamantes-Álvarez, M. A. Ponce-Camacho, O. Meza-Arballo, B. Valadez-Rivera and L. Casemiro-Oliveira	

### **Part III Connectivity and Novel Technologies**

<b>7</b>	<b>Blockchain Mechanisms as Security-Enabler for Industrial IoT Applications</b> .....	145
	J. Rian Leevinson, V. Vijayaraghavan and Muthu Dammodaran	
<b>8</b>	<b>Visible Light Communications in Industrial Internet of Things (IIoT)</b> .....	163
	Bugra Turan, Kadir Alpaslan Demir, Burak Soner and Sinem Coleri Ergen	
<b>9</b>	<b>The Internet of Things LoRaWAN Technologies in Academia: A Case Study</b> .....	193
	Lucio A. Rocha, Fernando Barreto and Laio O. Seman	

### **Part IV Applications and Use Case Scenarios**

<b>10</b>	<b>Implementation of Industrial Internet of Things in the Renewable Energy Sector</b> .....	223
	Somudeep Bhattacharjee and Champa Nandi	
<b>11</b>	<b>The Internet of Things in Health Care: Transforming the Industry with Technology</b> .....	261
	Wesley Doorsamy, Babu Sena Paul and Jerry Malapane	
<b>12</b>	<b>Internet of Things Applications and Use Cases in the Era of Industry 4.0</b> .....	279
	V. Vijayaraghavan and J. Rian Leevinson	
<b>13</b>	<b>Technology Trade-offs for IIoT Systems and Applications from a Developing Country Perspective: Case of Egypt</b> .....	299
	Aya Sedky Adly	
	<b>Index</b> .....	321

## About the Editor

**Prof. Dr. Zaigham Mahmood** is Published Author/Editor of twenty-seven books on subjects including electronic government, cloud computing, data science, big data, fog computing, Internet of things, smart cities, ambient intelligence, project management and software engineering, including: *Cloud Computing: Concepts, Technology & Architecture* which is also published in Korean and Chinese languages. Additionally, he is developing two new books to appear later in the year. He has also published more than 100 articles and chapters and organized numerous conference tracks and workshops.

He is Editor-in-Chief of *Journal of E-Government Studies and Best Practices* as well as Series Editor-in-Chief of the IGI book series on *E-Government and Digital Divide*. He is Senior Technology Consultant at Debesis Education, UK, and Professor at the Shijiazhuang Tiedao University in Hebei, China. He further holds positions as Foreign Professor at NUST and IIU in Islamabad Pakistan. He has served as Reader (Associated Professor) at the University of Derby, UK, and Professor Extraordinaire at the North-West University, Potchefstroom, South Africa. He is also Certified Cloud Computing Instructor and Regular Speaker at international conferences devoted to cloud computing and e-Government. His specialized areas of research include distributed computing, emerging technologies, project management and e-government.

# Contributors

**Aya Sedky Adly** Faculty of Computers and Information, Helwan University, Cairo, Egypt

**Fernando Barreto** Computer Systems Research Group, Department of Computer Engineering, Federal University of Technology—Paraná, Apucarana, PR, Brazil

**Somudeep Bhattacharjee** Department of Electrical Engineering, Tripura University, Suryamaninagar, India

**L. Casemiro-Oliveira** Universidade Federal Rural Do Semi-Árido—UFERSA, Mossoró, Brazil

**Turgay Çelik** MilSOFT Software Technologies, Ankara, Turkey

**Alina Chircu** Bentley University, Waltham, MA, USA

**Muthu Dammodaran** Infosys Limited, Bangalore, India

**Kadir Alpaslan Demir** Department of Software Development, Turkish Naval Research Center Command, Istanbul, Turkey

**Wesley Doorsamy** Department of Electrical and Electronic Engineering, University of Johannesburg, Johannesburg, South Africa

**Sinem Coleri Ergen** Department of Electrical and Electronics Engineering, Koc University, Istanbul, Turkey

**M. Cagri Kaya** Department of Computer Engineering, Middle East Technical University, Ankara, Turkey

**Ömer Köksal** ASELSAN Research Center, Ankara, Turkey

**J. A. López-Leyva** Center for Innovation and Design (CEID), CETYS University, Ensenada, Mexico

**Ricardo J. Machado** CCG/ZGDV Institute, Guimarães, Portugal;  
ALGORITMI Center, School of Engineering, University of Minho, Guimarães,  
Portugal

**Somayya Madakam** FORE School of Management, New Delhi, India

**Jerry Malapane** Department of Electrical and Electronic Engineering, University  
of Johannesburg, Johannesburg, South Africa

**O. Meza-Arballo** Center for Innovation and Design (CEID), CETYS University,  
Ensenada, Mexico

**Francisco Morais** CCG/ZGDV Institute, Guimarães, Portugal;  
ALGORITMI Center, School of Engineering, University of Minho, Guimarães,  
Portugal

**Champa Nandi** Department of Electrical Engineering, Tripura University,  
Suryamaninagar, India

**Halit Oguztuzun** Department of Computer Engineering, Middle East Technical  
University, Ankara, Turkey

**Babu Sena Paul** Institute for Intelligent Systems, University of Johannesburg,  
Johannesburg, South Africa

**M. A. Ponce-Camacho** Center for Innovation and Design (CEID), CETYS  
University, Ensenada, Mexico

**J. Rian Leevinson** Infosys Limited, Bangalore, India;  
Infosys Limited, Chennai, India

**Lucio A. Rocha** Computer Systems Research Group, Department of Computer  
Engineering, Federal University of Technology—Paraná, Apucarana, PR, Brazil

**Helena Rodrigues** CCG/ZGDV Institute, Guimarães, Portugal;  
ALGORITMI Center, School of Engineering, University of Minho, Guimarães,  
Portugal

**Mahdi Saeedi Nikoo** Department of Computer Engineering, Middle East  
Technical University, Ankara, Turkey;  
Spark Calibration Services, Ankara, Turkey

**Nuno Santos** CCG/ZGDV Institute, Guimarães, Portugal;  
ALGORITMI Center, School of Engineering, University of Minho, Guimarães,  
Portugal

**Michael L. Schwartz** Cal Lab Solutions, Denver, CO, USA

**Laio O. Seman** Computer Systems Research Group, Department of Computer  
Engineering, Federal University of Technology—Paraná, Apucarana, PR, Brazil

**Burak Soner** Department of Electrical and Electronics Engineering, Koc  
University, Istanbul, Turkey

**Eldar Sultanow** Capgemini Germany, Nuremberg, Germany

**A. Talamantes-Álvarez** Center for Innovation and Design (CEID), CETYS University, Ensenada, Mexico

**Bedir Tekinerdogan** Wageningen University, Wageningen, The Netherlands

**Bugra Turan** Department of Electrical and Electronics Engineering, Koc University, Istanbul, Turkey

**Takahiro Uchiya** Nagoya Institute of Technology, Nagoya, Japan

**B. Valadez-Rivera** Center for Innovation and Design (CEID), CETYS University, Ensenada, Mexico

**V. Vijayaraghavan** Infosys Limited, Bangalore, India



**Part I**  
**Concepts, Processes and Limitations**

# Chapter 1

## A Review of IoT Technologies, Standards, Tools, Frameworks and Platforms



Eldar Sultanow and Alina Chircu

**Abstract** In this contribution, we present an integrated view of the technologies, standards, tools, frameworks and platforms that support the end-to-end Internet of Things (IoT) solutions in general terms and highlight specific Industrial IoT (IIoT) solution components. Our study goes beyond existing research, including our own previous work, by focusing on all relevant IoT/IIoT solution components relating to development and operation. Specifically, we discuss the communication standards, messaging protocol standards, and communication platforms; device control, integration and simulation frameworks; tools and frameworks for modeling, development and deployment; and IoT cloud integration platforms that support IoT solutions. By highlighting the features as well as the advantages and limitations of different IoT solutions, this technical analysis can prove useful to IoT practitioners designing IoT and IIoT systems with diverse requirements; to students further learning about IoT/IIoT vision; and to researchers interested in understanding the current limitations of the IoT/IIoT landscape and developing new standards, tools, frameworks and platforms for future application.

**Keywords** Internet of things · IoT · Industrial IoT · IIoT · Reference architecture · IoT development · Standards · RAMI 4.0 · Industry 4.0

### 1.1 Introduction

The Internet of Things (IoT), a term coined in the 1990s in the context of supply chains [1], is one of the most exciting technology developments today. It promises to embed sensors into physical things (personal devices, industrial machines, vehicles, appliances, and the like) and enable them to record, process, and communicate their status data (position, movement, temperature, operating status, errors, etc.) with other

---

E. Sultanow  
Capgemini Germany, Bahnhofstraße, 11C, 90402 Nuremberg, Germany  
e-mail: [eldar.sultanow@capgemini.com](mailto:eldar.sultanow@capgemini.com)

A. Chircu (✉)  
Bentley University, 175 Forest Street, Waltham, MA 02452-4705, USA  
e-mail: [achircu@bentley.edu](mailto:achircu@bentley.edu)

© Springer Nature Switzerland AG 2019  
Z. Mahmood (ed.), *The Internet of Things in the Industrial Sector*, Computer Communications and Networks, [https://doi.org/10.1007/978-3-030-24892-5\\_1](https://doi.org/10.1007/978-3-030-24892-5_1)

*things* or with Internet servers (directly or through gateways) for further processing. The IoT market size is predicted to reach many hundreds of billions of dollars by 2020, with the USA, China, Germany, and UK leading the growth [2].

The Industrial IoT (IIoT), also known as the Industrial Internet, the Internet of Industrial Things, and Industry 4.0, focuses on the IoT technologies that connect industrial machines among themselves and to the Internet. This enables automated instrumentation, reporting, and even manufacturing [3, 4]. With 2.6 billion connections between industrial machines predicted by 2020, IIoT is one of the top growth sectors in the IoT scenario [2, 5], leading to an expected market size of over \$100 billion by 2020 [5]. The top industries anticipated to benefit from the IIoT vision are discrete manufacturing, transportation, logistics and supply chains, utilities such as electricity, and health care [3–9]. IIoT applications related to smart factories, smart warehousing, predictive and remote maintenance, freight, goods and transportation monitoring, smart utility metering, smart grids, smart cities, smart farming, live-stock monitoring, asset tracking and performance management, industrial environment monitoring, safety and health monitoring, and many others, are predicted to become more efficient and productive and, in turn, enable digital transformation in companies, in fact the entire industries [3, 10, 11].

While IoT and IIoT share the same basic building blocks including technologies, the need for integrated solutions is much more acute in the IIoT space, where standards, interoperability, and integration with legacy technologies are some of the most important factors for successful technology development, implementation, management, and adoption [3, 5, 8, 12, 13]. Not surprisingly, leading global companies such as Bosch, Dell, GE, Huawei, IBM, Siemens, Mitsubishi, Cisco, China Mobile, Boeing, Intel, SAP, Ericsson, and many others are taking an active interest in defining standards, best practices, and processes through IIoT consortia and other collaboration initiatives (as described in the next section).

In this chapter, we present an integrated view of the technologies, standards, tools, frameworks and platforms that support end-to-end IoT (and the subset of IIoT) solutions. We build on our ongoing research focusing on specific industries (pharma, health care, and life sciences) and generic architectural frameworks [14, 15]. In particular, we significantly extend our recent work on an integrated IoT reference architecture [16]. The chapter's novel contribution is a detailed discussion of the components necessary for a complete IoT solution and how they fit into the IoT development, implementation, and management ecosystem. The need for such an approach has been advocated by many other IoT researchers [5, 8, 12, 13]. While simpler analyses of individual IoT components have been published (see, for example, [13]), to our knowledge, no other authors have discussed all the different technologies, standards, tools, frameworks and platforms that support an end-to-end IoT solution in the same paper. Thus, this book chapter can serve as a reference for practitioners developing new IoT solutions. It can also help researchers identify unmet needs and design improved or novel IoT technologies, standards, tools, frameworks and platforms.

This chapter covers several important topics including: architectures and frameworks; communication protocols and device connectivity; and sensors and actuators,

among others. The chapter is organized as follows: Sect. 1.2 examines the related work, Sect. 1.3 presents the analysis of IoT technologies, standards, tools, frameworks and platforms, and Sect. 1.4 presents the conclusions and suggestions for future research.

## 1.2 Related Work

Industrial Internet of Things (IIoT) is the application of IoT technologies to industrial settings such as manufacturing. Based on a review of existing research, IIoT can be defined as *a system comprising networked smart objects, cyber-physical assets, associated information technologies, and optional cloud or edge computing platforms, which enable real-time, intelligent and autonomous access, collection, analysis, communication, and exchange of process, product and/or service information, within the industrial environment, so as to optimize overall production value. This value may include: improving product or service delivery, boosting productivity, reducing labor costs, reducing energy consumption, and reducing the build-to-order cycle* [17]. IIoT is closely related to the Industrie 4.0 (or Industry 4.0) concept promoted by the German government as a way of developing the German economy through a fourth industrial revolution (Industry 4.0) [17–19]. The Industry 4.0 definition emerging from published research is *an integrated adapted, optimized, service-oriented, and interoperable manufacturing process which is correlated with algorithms, big data, and high technologies* [20]. Other related concepts include cyber-physical systems (which combine physical objects and processes with real-time data collection and autonomous digital monitoring and control capabilities), and smart factories or cyber-physical production systems (which are autonomously controlled flexible manufacturing facilities) [17–20].

Over the last few years, researchers and practitioners alike have become more interested in developing reference architectures for IoT and IIoT [18, 19]. Such frameworks describe the necessary components for building integrated end-to-end IoT solutions in general, or building industry-specific IIoT applications.

Generic architectures usually organize the components necessary for building IoT solutions in several distinct layers. Lin et al. [21] present a four-layer architecture (including perception, network, service, and application layers), describe key technologies and standards in each layer, analyze security and privacy issues, and propose a way of processing the IoT data using fog/edge computing. Similarly, Xu et al. [22] discuss a four-layer architecture (including sensing, networking, service, and interface layers) as well as key enabling technologies and key applications for industries such as health care, food supply chains, and transportation and logistics, among others. Specific architectures are also being developed in many areas, including those relevant for IIoT such as health care, manufacturing, transportation, and logistics.

In the healthcare domain, Pang et al. [23] propose an architecture for in-home healthcare devices that includes sensors, network connections to an in-home health-

care system, and cloud connections to other information systems such as hospital systems. Ramirez et al. [24] describe an IoT architecture for sensory impaired individuals, where sensors, actuators, and monitoring devices such as mobile phones and tablets can transmit data over wired or wireless networks to dedicated applications that interpret the data and intelligently respond to user needs. Dhariwal and Mehta [25] propose a 3-layer architecture for a smart hospital that includes a perception layer (which collects data from patients, doctors, and nurses and transmits this data to network), a network layer (which transmits real-time data within the network and integrates various sources of data), and an application layer (which manages hospital operations, equipment, finances and provides decision support based on analysis of data about diseases, patients, clinics, department, medicines, etc.).

In the manufacturing domain, Zhang et al. [26] propose a generic architecture to attach sensing capabilities to various resources in a manufacturing environment, capture data in real time during the production process, filter, and process data into meaningful metrics, and provide real-time analysis and feedback based on the data. Zancul et al. [27] develop an architectural model relevant for product–service systems and identify key IoT impacts in processes such as remote machine setup, maintenance (both corrective and predictive), supply chains, product pricing, and information reporting.

Other researchers focus on IoT architectures from a specific functionality perspective, such as energy-efficient IIoT [28] or secure IoT [29, 30]. Last, but not least, there are also efforts to define parts of IIoT architectures, such as analytical frameworks for describing the IIoT devices [17].

On the practitioner side, IIoT communities of interest and reference models are also proliferating. For example, the Industrial Internet Consortium (IIC) has defined the Industrial Internet Reference Architecture (IIRA), a standard-based open architecture for IIoT systems applicable across many industries (e.g., energy, health care, manufacturing, transportation, etc.) [31].

IIRA includes four viewpoints: business (focused on identifying the business stakeholders and their vision, values and objectives), usage (focused on the expected system use), functional (focused on the functional components of the system and their interconnections), and implementation (focused on technologies that support the functional components).

Industrial Internet Consortium (IIC) has developed an Industrial Internet Connectivity Framework (IICF), which organizes connectivity technologies into a stack model and proposes achieving interoperability among various standards through gateways [31].

In the Industry 4.0 area, Platform Industrie 4.0 has developed the Reference Architecture Model for Industrie 4.0 (RAMI 4.0) which is a detailed service-oriented architecture for manufacturing. It focuses on several axes: factory (which defines how products and manufacturing systems interact in an enterprise), product life cycle (which captures the development, production, maintenance, usage and end of life stages of a product), and architecture (based on six layers describing both the real and digital world) [31].

While IIRA and RAMI 4.0 each have a different focus (broad industry applicability versus manufacturing only), efforts to compare and map their components to each other are already underway in order to ensure interoperability between different IIoT systems built on these two different architectures [31].

Major technology providers, such as IBM, are also active in the IoT architecture area, proposing both general and specific reference architectures for IoT and IIoT [32]. IBM's IoT reference architecture consists of five layers (user, proximity network, public network, provider cloud, and enterprise network) and has applicability to multiple industries. IBM's Industrie 4.0 reference architecture is specific to manufacturing and consists of three manufacturing-specific layers: edge, plant, and enterprise [32].

In addition, several other organizations are involved in developing IIoT standards and tools that can be used to build IIoT systems. The Object Management Group (OMG) has developed the Data Distribution Service (DDS) standard, which is promoted as *the first open international middleware standard directly addressing publish/subscribe communications for real-time and embedded systems*, which makes it ideal for *high-performance, highly scalable Industrial Internet of Things (IoT) and large-scale Consumer IoT application environments which require real-time data communication exchange* [33]. The Open Connectivity Foundation is focused on IoT device interoperability for consumers, businesses and industries and on *delivering a standard communications platform, a bridging specification, an open-source implementation and a certification program allowing devices to communicate regardless of form factor, operating system, service provider, transport technology or ecosystem* [34]. The Internet of Things Consortium (IoTC) is focused on IoT ecosystem interoperability and usability, data openness and security, and market development and provides information on IoT use cases, IoT hardware and software, as well as IoT vendors [35]. Last, but not least, the Eclipse Foundation, a nonprofit organization where individual developers and companies from many industries collaborate on open-source projects (providing runtimes, tools, and frameworks for many domains), has emerged as a major IoT player over the last few years. Its Eclipse IoT Working Group involves companies such as Bosch, Huawei, IBM, Intel, Nokia, SAP, and Siemens and has generated many relevant open-source projects for the IoT landscape [36].

### 1.3 Analysis

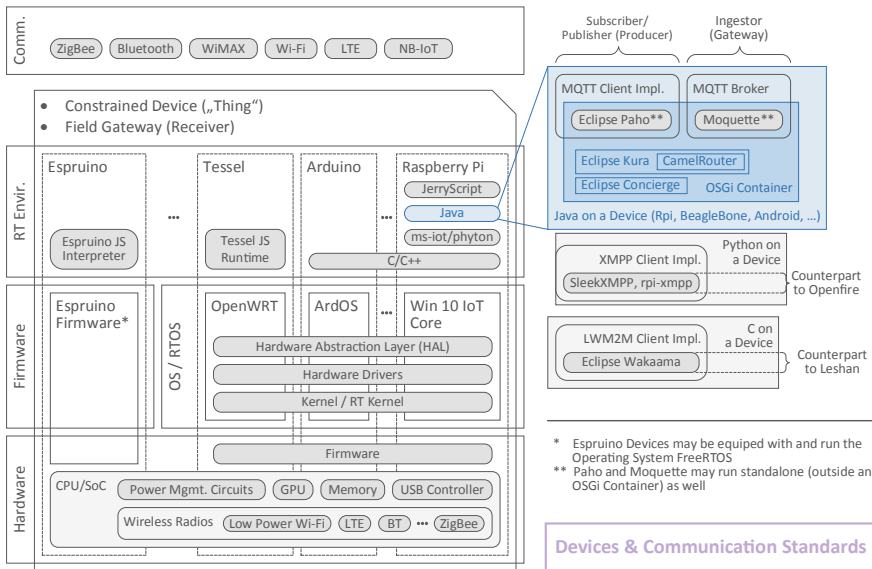
Our review of current research reveals that the existing architectures provide only a partial overview of the components necessary for developing an end-to-end IoT solution. It is usually just for sensing and networking technologies (in generic models) and just for industry-specific functionality (in specific models). To address this gap, we developed an integrated IoT reference architecture [16] focusing on the entire IoT life cycle, from IoT application development to operations (solution in action). Our proposed architecture senses the environment and collects data through IoT-

enabled smart devices, transmits it through communication standards, protocols and platforms, processes it using back-end systems, and uses it in front-end applications. Figures 1.1, 1.2, and 1.3 illustrate a detailed graphical representation of the reference architecture, organized in three components:

- devices and associated communication standards—refer to Fig. 1.1
- protocols, back end, and front end as presented in Fig. 1.2
- development platforms as shown in Fig. 1.3.

Taken together, Figs. 1.1 and 1.2 depict the necessary elements for an IoT end-to-end solution, which can be visualized as a stack consisting of a bottom layer describing the devices (hardware, firmware, and runtime environment), a layer of communication standards (as shown in Fig. 1.1), and layers of messaging protocol standards, back-end and front-end tools, frameworks and platforms (as shown in Fig. 1.2). Figure 1.3 depicts development platforms that address the description and integration of the devices shown in Fig. 1.1, as well as the setup of the back-end platforms and the development of IoT applications shown in Fig. 1.2. Interested readers should refer to our existing research [16] for an explanation of how the reference architecture was developed.

In this chapter, we extend our previous work [16] by analyzing the various IoT technologies, standards, tools, frameworks and platforms included in our architecture. These include connected devices, communication standards, messaging protocol standards, communication platforms, device control, integration and simulation frameworks, tools and frameworks for modeling, development and deployment, and



**Fig. 1.1** Reference architecture for IoT—devices and communication standards. Adapted from [16]

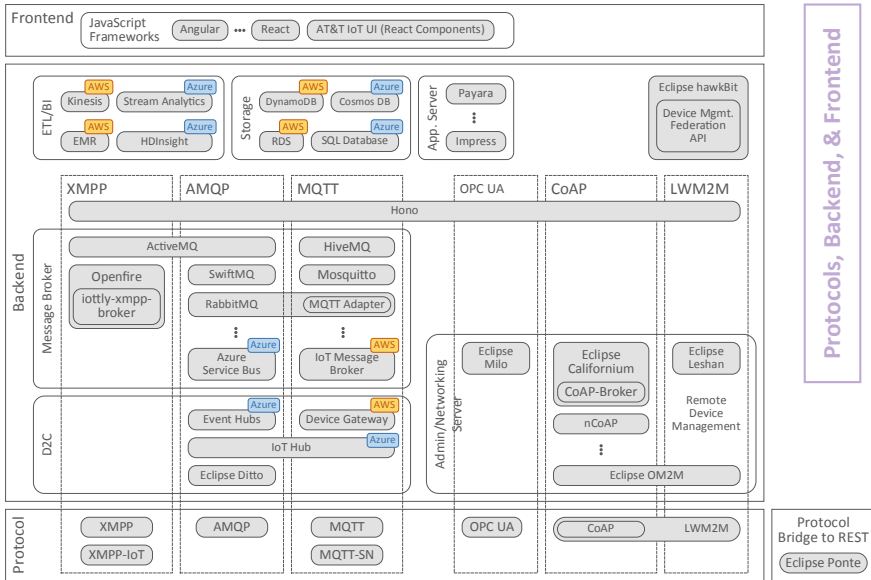


Fig. 1.2 Reference architecture for IoT—protocols, back end, and front end. Adapted from [16]

IoT cloud integration platforms. When appropriate, we also highlight specific IIoT solution components. We focus our analysis on characteristics relevant for developers and researchers interested in choosing one option over another (for example, bandwidth, energy consumption, security for standards, or specific technical features for platforms and frameworks), and present advantages and disadvantages as applicable.

### 1.3.1 IoT Devices

IoT devices, or *things* in the IoT, are the first building block of the IoT infrastructure. Any physical object (including human users of the IoT) can become IoT-enabled with the addition of IoT hardware that provides functionality ranging from simple sensing abilities to more sophisticated processing and networking capabilities. IoT hardware includes both embedded systems and boards (such as Arduino, Raspberry Pi, Tessel, Espruino, Pinoccio, Beaglebone Black, and others) and stand-alone devices (such as Samsung Gear or FitBit in the consumer-things space) [37]. Embedded systems consist of a microcontroller (with one or more processors, memory, graphics processing unit, general-purpose input/output interfaces, and specific interfaces such as wireless networking, camera, or USB) as well as other parts (such as a power source, sensors for light, heat, motion, sound or other environmental inputs, analog-to-digital and digital-to-analog converters, various actuators, motors, smart materials,



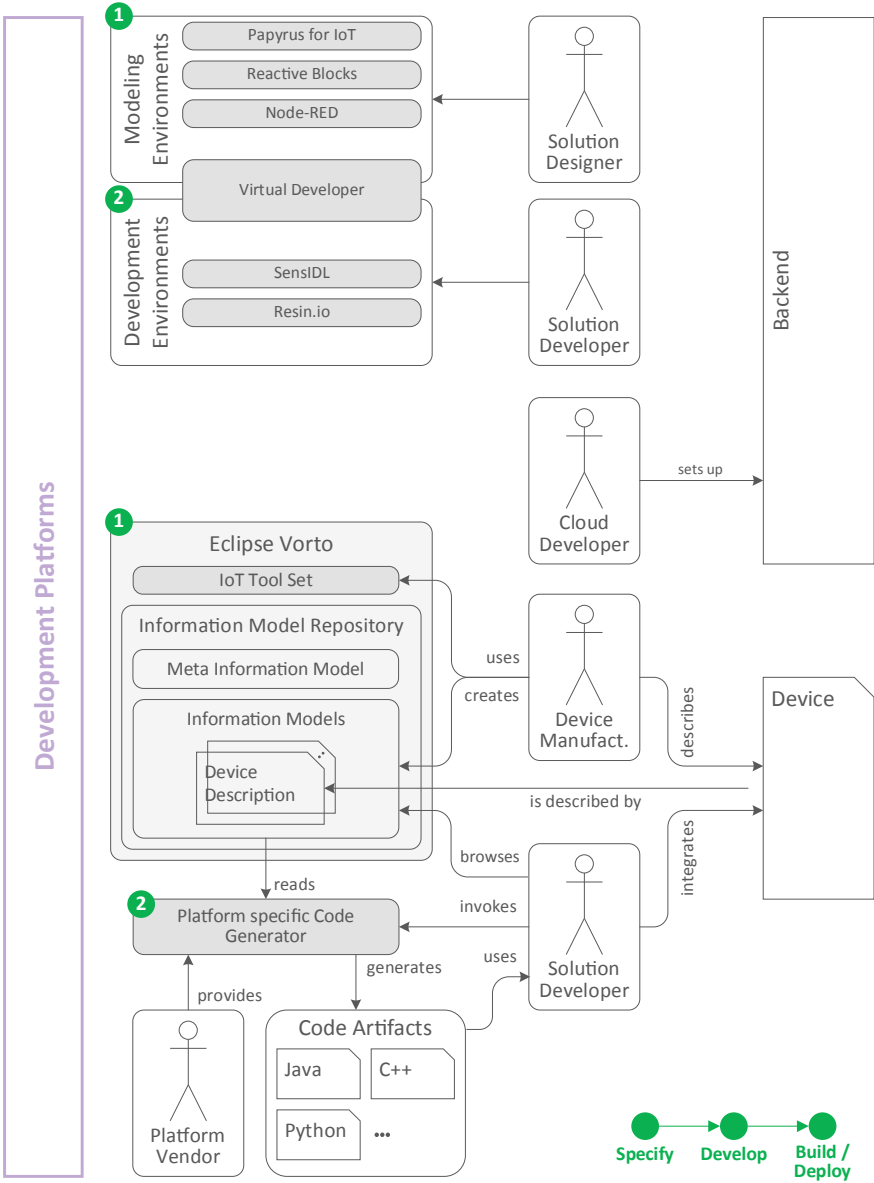


Fig. 1.3 Reference architecture for IoT—development platforms. Adapted from [16]

and devices that can control the environment usually by converting a source of energy into motion).

In this context, many different systems exist; and IoT designers can choose the best platform for a specific application based on a variety of factors. Interested readers can consult the most recent detailed comparisons provided by Singh and Kapoor [37], which is based on data collected in 2017.

### 1.3.2 *Communication Standards*

Communication standards are essential for enabling IoT devices to reliably communicate with each other and with other entities on the Internet. A comparison of the most widely used communication standards based on current practitioner analyses [38–45] is presented in Table 1.1.

One of the most widespread communication standards is Wi-Fi (or WiFi), which is a wireless local area network (WLAN) standard defined by IEEE 802.11 specification. This standard enables connections directly with a server, such as in the case of Sonoff WiFi Power Switches, which can send their readings of energy consumption directly to the OpenWrt Router [38]. OpenWrt is a Linux distribution for embedded systems like WLAN Router (e.g., Linksys provides such a router with WRT3200ACM which is enabled with OpenWrt Open Source).

Another standard is ZigBee, an IEEE-802.15.4 specification for wireless personal area networks well-suited for low-power devices and for building automation, sensor networks, and light technology applications. Although ZigBee's focus is on short-range networks, bigger ranges up to several kilometers are still possible.

Bluetooth is another standard (based on IEEE 802.15.1 specifications) for data transfer between devices over short distances. Typical deployment areas are mobile loudspeakers, connections between a smartphone and PC or between a smartphone and an onboard computer in a car, or wireless mouse and keyboard connections to a computer.

There is also the WiMAX/IEEE-802.16 standard, which is used for example by Sigfox and LoRa [39] and popular mobile standards like LTE—the fourth generation (4G) high-speed mobile communication standard. For a long time, the mobile phone industry did not show any interest in industrial wireless IoT applications, but the 3GPP (3rd Generation Partnership Project—the worldwide cooperation of standardization bodies for mobile industry) has, for the first time, standardized variations such as NB-IoT specifically for machine-to-machine (M2M) wireless communication. NB-IoT, which stands for Narrowband IoT, is a new wireless standard used, among others, for smart gas and water meters and for smart city applications (management of street lights, intelligent parking guidance systems, etc.) [40]. NB-IoT is similar to LTE-M, another cellular IoT standard designed for low-power, low-range applications [41].

Other emerging communication standards include LoRa, Sigfox, WAVIoT, DASH7, LTE-M (LTE M2M), NB-LTE-M, Weightless, 6LoWPAN (IPv6 over LWPAN), Z-Wave, Symphony, and Wavenis [42].

**Table 1.1** Comparison of IoT communication standards (based on [38–45])

Standard	Frequency range	Data rate	Bandwidth	Coverage	Energy need	Advantages	Disadvantages
Wi-Fi	2.4–5.9 GHz Bands	Variable; 1.5–54 Mbps (IEEE 802.11a-1999 specification), but higher data rates up to 7 Gbps possible (see for example the IEEE 802.11ad specification)	Variable, up to 450–600 Mbps for 2.4 GHz Wi-Fi and up to 1300 Mbps for 5 GHz Wi-Fi	50–100 m	High energy need	Very simple setup, most robust security available to date, transparent implementations, multiple clients can connect to an access point simultaneously (depending on the max allowed for device), very high data rates, de facto standard for wireless Internet connectivity worldwide	Hotspots require a lot of power (i.e., constant energy source), adapters and drivers require memory and processing resources unavailable in simple appliances, and signals cannot go through walls without losing strength thus limiting range to within a building

(continued)

**Table 1.1** (continued)

Standard	Frequency range	Data rate	Bandwidth	Coverage	Energy need	Advantages	Disadvantages
ZigBee	2.4 GHz	250 Kbps	2 MHz	50 m, several km possible	Low energy need	Low-power consumption; smart time allocation for fixed bandwidth communications, low cost, low latency (< 30 ms for device discovery, 15 ms for wake-up and 15 ms for active channel access) can be used to create large networks with up to 254 devices connected to a master, implements AES-128 for data encryption and security	Short range and low data transfer speed

(continued)

**Table 1.1** (continued)

Standard	Frequency range	Data rate	Bandwidth	Coverage	Energy need	Advantages	Disadvantages
Bluetooth	Variable (2402–2480 MHz or 2400–2483.5 MHz) including guard bands 2 MHz wide (bottom) and 3.5 MHz wide (top)	Depends on standards: BT 3 & 4 up to 24 Mbps; BT 2 up to 3 Mbps; BT 1 up to 700 Kbps	Up to 1 Mbps (BT 4)	1–100 m (typical 10 m)	Medium to very low; BT 4 Bluetooth Low Energy (BLE) has very low energy need	Widely used standard makes it convenient to connect various devices, cost-effectiveness makes implementation in low-end devices possible, very easy and convenient to use, BLE paves the way for more possibilities as its low energy needs make it suitable for more low-power devices	Security concerns (devices can be hacked into easily), only one ongoing connection at a time, limited in range (ideal only for communication within a room, more range requires a lot more power), BLE bandwidth capability limited and transfer rate lower

(continued)

**Table 1.1** (continued)

Standard	Frequency range	Data rate	Bandwidth	Coverage	Energy need	Advantages	Disadvantages
WiMAX	2–11 GHz	124 Mbps	Adjustable 1.25 M to 20 MHz	30–50 km	High energy need	Long range; symmetrical bandwidth over long range; hundreds of users can be served from a single WiMAX station; operates on an unlicensed spectrum of frequency	Serving lots of clients results in poor bandwidth; can be affected by weather conditions, high latency, line-of-sight required for longer range, signal prone to distortion due to noise

(continued)

Table 1.1 (continued)

Standard	Frequency range	Data rate	Bandwidth	Coverage	Energy need	Advantages	Disadvantages
LTE	Variable; in Germany, the LTE frequencies in the 800 MHz, 1800 and 2600 MHz ranges are used for the 4G mobile radio	Variable; usually 100 Mbps (download), 50 Mbps (upload)	Variable; 100 Mbps	Variable; 2–10 km; 30 or 75 km possible (Australia)	Low energy need	High speed (due to increased bandwidth) is advantageous for mobile devices; more coverage than other systems such as WiFi, which forces users to depend upon hotspots in each area they visit; 4G networks offer complete privacy, security, and safety	Connectivity is still limited to certain specified carriers and regions; new equipment would have to be installed in order to supply LTE services—however, the hardware compatible with 4G networks is available at much cheaper rates today than in the past

(continued)

**Table 1.1** (continued)

Standard	Frequency range	Data rate	Bandwidth	Coverage	Energy need	Advantages	Disadvantages
NB-IoT	LTE in-band, guard band, stand-alone; in Europe, Telekom will use 800 and 900 MHz frequencies	250 Kbps	180 kHz	Gains of 20 dB over LTE; covers distance of less than 22 km	Low energy need (10-year battery life)	Low-power consumption (expected) moderate module costs, physical infrastructure already in place, ensuring fast rollout and market readiness, telco provided, proved ability to provide mass mobile networks with high service level	Less coverage than leading standards (Europe), less roaming support (2G sunset and available LTE infrastructure may boost licensed standards), early adoption/not yet mature; pricing models evolving; hard to build business case; no voice transmission support



### 1.3.3 Messaging Protocol Standards

Messaging protocols define the syntax and semantics of the data being transferred between IoT devices and servers. They focus on delivering entire messages, rather than on just transferring data without worrying about its meaning, as communication standards often do. Table 1.2 provides a comparison of most widely used protocol standards based on current practitioner analyses [46–57]. A brief description of these protocols is also provided below.

MQTT (Message Queuing Telemetry Transport) is an IoT messaging protocol introduced in 2011 that is maintained and enhanced by the independent Organization for the Advancement of Structured Information Standards (OASIS). It is highly efficient and scalable (up to several hundred thousand clients per server) and has a very small protocol overhead. MQTT implements a publish/subscribe messaging model on top of the widely known TCP/IP standards. It is specifically designed for machine-to-machine (M2M) use cases and provides reliable transfer of messages over unreliable (such as mobile or limited bandwidth) networks and for the high-performance deployment of IoT devices with low memory and lower processing power [46]. It is useful in the automobile industry (for connected cars), in the energy sector as well as in the field of building automation. Since 2016, MQTT is also an ISO standard (ISO/IEC 20922). The requirement to use an existing network such as TCP/IP limits the application of MQTT to devices that can support such a network. To address this limitation, MQTT-SN (MQTT for Sensor Networks) was developed as a version of MQTT designed specifically for wireless sensor networks (consisting of very simple, low-cost devices with limited power, processing, and storage capabilities) and their characteristics (high failure rates, lower transmission rates, shorter message lengths) [47]. Originally implemented on top of the ZigBee open communication standard, MQTT-SN is in fact designed to work on any underlying network. It is very close to MQTT but has several differences that enable it to support shorter message lengths and lower bandwidths [47].

AMQP (Advanced Message Queuing Protocol) is an open standard for a communication protocol between a client and a message broker, or between various message brokers. AMQP-enabled brokers include, for example, RabbitMQ, Apache ActiveMQ, Apache Qpid, SwiftMQ, Microsoft Azure Service Bus, and Red Hat Enterprise MRG. AMQP was created by a consortium of software companies and financial institutions, which include Microsoft, Red Hat, Cisco, Bank of America, Goldman Sachs, Credit Suisse, and many others. Microsoft has integrated the AMQP protocol directly into its Azure cloud solution.

XMPP (eXtensible Messaging and Presence Protocol), formerly known as Jabber, is an XML-based communication protocol frequently used by instant messengers for chat applications. It is less used in the field of IoT due to large protocol overheads caused by XML [46] and has even been phased out of chat applications (such as in the case of Facebook). XMPP has enhancements designed especially for IoT use cases. These, however, are supported by very few servers and clients. The GitHub-project XMPP-IoT provides a collection of such enhancements, including sensor discovery

**Table 1.2** Comparison of IoT messaging protocol standards (based on [46–57])

Standard	Architecture	Underlying transport layer	Communication	Overhead	Security	Advantages	Disadvantages
MQTT	Asynchronous message exchange	TCP	Unicast	Small	Optional TLS, simple user-name/password authentication, SSL for data encryption	Minimal protocol overhead, several hundreds of thousands of clients per server, features designed for IoT use cases, suitable for resource-limited devices, client implementations available for all common languages	Pure request/response architectures can only be implemented in MQTT with additional effort, since it uses TCP connections to a MQTT broker, an always-on connection will limit the time the devices can be put to sleep
MQTT-SN	Asynchronous message exchange	Any	Unicast, multicast	Small	Optional TLS	Many-to-many communication protocol, credibility—supported by IBM, Eurotech, Cisco and Red Hat, open nature, open source	Lacks support for labeling messages, making it difficult to understand, must be familiar with the message formats to enable communication

(continued)

Table 1.2 (continued)

Standard	Architecture	Underlying transport layer	Communication	Overhead	Security	Advantages	Disadvantages
AMQP	Asynchronous message exchange	TCP	Unicast, multicast	Large	SASL authentication, TLS for data encryption	Many possibilities for message delivery (beyond Pub/Sub) suitable for broad range of messaging-middleware infrastructures and peer-to-peer data transfer	Overhead (smallest packet size 60 bytes) affects the expended effort in a large number of devices and messages, not easy to implement
XMPP	Synchronous message exchange	TCP	Unicast, multicast	Large	TLS and SASL	Clients available in many programming languages, many features, many optimized for instant messenger use cases	High protocol overhead, high fragmentation of server and client features, no end-to-end encryption, no QoS functionality

(continued)

**Table 1.2** (continued)

Standard	Architecture	Underlying transport layer	Communication	Overhead	Security	Advantages	Disadvantages
CoAP	REST; layered approach	UDP	Unicast, multicast	Medium	Optional DTLS	Very efficient, URI and content-type support, open standard, designed for web interoperability, easily translates to HTTP, easy migration from HTTP, can be used on top of a variety of different packet-based communication protocols	Challenges of Network Address Translation (NAT) through UDP, few client and server implementations, 1-to-1 protocol—broadcast capabilities not native, best suited for devices that support UDP or a UDP analog
HTTP	REST; layered approach	TCP	Unicast	Large	Typically based on SSL or TLS	Libraries for almost all programming languages available, easy to learn.	High protocol overhead, no server push communication natively possible (only by means of long polling, server sent events or WebSockets), no possibility to map 1/N communication

(continued)

**Table 1.2** (continued)

Standard	Architecture	Underlying transport layer	Communication	Overhead	Security	Advantages	Disadvantages
OPC UA	Service-oriented architecture (SOA); layered approach	TCP, UDP also possible	Unicast, multicast	Medium	Integral part of specification and communication stacks, OAuth 2.0, exchange of certificates for identification of application instances, SSL/TLS, WS Secure Conversation (UA XML), UA Secure Conversation (UA Binary)	Many features, open source, addresses security comprehensively, defines communications from the application to the transport layer making it very interoperable between vendors, interoperability to the device and enterprise levels	Not easy to implement, primarily beneficial for tying PLC and sensor data into existing industrial applications like SCADA and MES systems, where OPC and OPC UA connectivity are already available
LWM2M	REST; layered approach	CoAP over UDP, TCP and SMS, LWM2M over MQTT possible	Unicast, multicast	Small	Secure communications between client and server using DTLS	Very flexible in utilization of underlying transport layer, widely used and established standard for remote device management, supports both powerful embedded devices and low-power ones	Implementation dependent on CoAP, needs CoAP expertise, data model is flat and simple (no complex trees) (this might be also considered as an advantage)

in sensor networks, efficient multicasting of sensor data, efficient data compression, interacting with humans and systems via chat messages, and many others [54].

CoAP (Constrained Application Protocol) is often described as the *HTTP for IoT*. It implements the request/response pattern—the most basic and widespread of the client–service interaction patterns. CoAP is more efficient than HTTP as the protocol is binary including all the headers and is thus suitable for energy-constrained wireless sensor networks. However, it lacks security features, requiring additional protocols for securing the network [55].

HTTP (Hypertext Transfer Protocol), the bedrock of all protocols, is still the first choice for request/response-based IoT communication [46]. Due to very high protocol overheads (since HTTP is completely text-based), it is rather unsuitable for use cases where the volume of data transferred matters (for example if mobile/bandwidth-constrained networks are involved). Furthermore, the request/response model allows 1-to-1, but not 1-to-many communication. Therefore, HTTP is also not suitable when a message has to be sent to several recipients simultaneously.

OPC UA (Open Platform Communications Unified Architecture) is an industrial M2M communication protocol based on AMQP which can securely and reliably transport machine data (control variables, measured values, parameters) as well as semantically describe this data in a machine-readable way. It is a de facto standard in the automation field and is set for wide adoption in industrial IoT applications. It is most successful for Supervisory Control and Data Acquisition (SCADA) systems and is considered heavier than the publish/subscribe-oriented MQTT. However, OPC UA is enhanced in real time with a publisher/subscriber mechanism [56].

LWM2M (Lightweight M2M) is a messaging protocol designed by the Open Mobile Alliance (OMA) based on CoAP for managing IoT devices. It defines the interfaces for bootstrapping, device discovery, registration, and device management. It supports parameterization and monitoring of devices as well as the update of firmware. LWM2M also supports the communication between servers (nodes in a private or public network) and clients (embedded in a device).

As messaging protocol standards with different characteristics (message size, overhead, power consumption, bandwidth, reliability, security, etc.) proliferate, protocols need to be carefully evaluated in order to determine their fit for a particular IoT application [57].

### 1.3.4 Communication Platforms

In order for the protocols defined in the previous section (such as AMQP, MQTT, and XMPP) to be implemented in practice, it is necessary to define the procedures through which many IoT devices can communicate with other devices or with servers in an organized manner. Most communication platforms use a broker model, which provides trusted message prioritization, routing, filtering and delivery between a publisher and a subscriber [50]. Platforms can be configured as a centralized broker system (with all messages going through one server), a centralized multibroker sys-

tem (with several brokers on different servers, each with its own message queue), or a decentralized broker system (which has no central server and uses the IP multicast protocol coupled with local client-side functionality for persistence, security, and transactions) [50]. We present examples of such brokers below.

HiveMQ is an Enterprise MQTT Broker conceptualized for commercial use, developed in Germany by dc-square GmbH. The broker supports the publish/subscribe MQTT standard. It has a cluster functionality to scale HiveMQ deployments (supporting millions of MQTT clients on different machines) in a horizontal linear manner [58]. Developers can implement their own mechanisms for cluster discovery.

An alternative for HiveMQ is the open-source implementation Mosquitto—an open-source MQTT broker. Mosquitto is written in C and is a project of the Eclipse IoT Working Group, which includes Bosch, Red Hat, and SAP [59]. Mosquitto also runs on a Raspberry Pi device.

Another open-source MQTT broker written in Java is Moquette. Like Mosquitto, it also runs on IoT devices such as on a Raspberry Pi [60]. Usually, Moquette runs stand-alone. However, it can also be integrated into an OSGi container like Concierge [61] or Kura [62].

Another alternative is Pivotal RabbitMQ, an open-source message broker. While not developed specifically for MQTT, it has an MQTT adapter, thus offering a full-fledged open-source MQTT broker as well [63].

The Eclipse Paho project provides open-source client implementations of MQTT and MQTT-SN messaging protocols which are aligned with the new, existing, and future IoT applications. The word Paho comes from the Maori language and means to distribute or send. Paho is a broadcast messaging protocol for IoT. An MQTT solution is often used by means of Paho (publisher and subscriber on client side) and Mosquitto (broker on server side). Paho is set up as a standard messaging library in the OSGi container Eclipse Kura [64].

### ***1.3.5 Device Control, Integration, and Simulation Frameworks***

IoT solutions usually involve a diversity of IoT devices interacting with each other and transmitting data to IoT-based applications. The device control, integration, and simulation frameworks enable easy configuration of these devices and efficient management of their operation. We present examples of such frameworks below.

The Java-based framework openHAB (open Home Automation Bus) integrates buildings automation components from different manufacturers in a single device-independent and protocol-independent platform [65]. openHAB is continuously adding bindings (which describe how to transport data in and out of a device) for end devices, such as Xiaomi Mi smart home devices, IKEA Trådfri smart lighting devices, and Gardena's smart garden robotic lawn mowers [66, 67]. The technology-specific

bindings communicate internally with the openHABCore via the openHAB event bus. However, the external communication of openHAB with the outside world takes place via an MQTT broker such as HiveMQ [66]. OpenHAB builds on the Eclipse SmartHome project [66, 68] and is also connected to the Eclipse IoT Market, where developers can find a connection to devices which are not included in openHAB (if there are no open-source implementation or suitable licenses) [66]. There is also a self-configuring Raspberry Pi setup called openHABian, which starts with an SD card image and automatically installs Java, openHAB, Samba, and other software. Industry giants like Z-Wave, KNX, Homematic, EnOcean and Insteon are already integrating their smart home products (such as smart lights, thermostats, alarm systems, etc.) with openHAB in order to ensure smooth connectivity of their various devices in smart home applications.

The Eclipse Edge project falls under the Apache license 2.0 and provides a hardware abstraction Java API (application programming interface) for accessing hardware features of microcontrollers such as the general-purpose input/output (GPIO) interfaces [69]. As the smallest common point of Java SE, Java SE Embedded, MicroEJ and Android, the Edge Device Configuration (EDC) provides a minimal execution environment (which covers Java standard packages `java.lang`, `java.util` and `java.io`) for a device compatible with Edge. Minimum requirements are a 32-bit processor with a frequency of 16 MHz, 32 KB RAM and a 128 KB flash memory [69].

Eclipse Ditto [70] provides access to digital twins (software abstractions of real-world devices) and mediates between the physical world and the digital twin representations. Digital twin is an IIoT solution that can be useful in understanding past and current performance of real-world machines, optimizing the operation of the machines, and predicting future operation and maintenance needs. Core aspects of the Eclipse Ditto framework include device-as-a-service (a higher abstraction level of the device in the form of an API, which is used to work with this device), state management of digital twins (in terms of current state data as well as configuration properties), and organization of the digital twins (geographic assignment and tracking of their geographical relationship, metadata assignment, and search functions) [70].

### ***1.3.6 Tools and Frameworks for Modeling, Development, and Deployment***

The development life cycle of IoT applications (specifying, modeling and developing the system, and deploying it in production mode) is supported by specific tools and frameworks, which we review below.

Eclipse 4diac is an Open-Source PLC (Programmable Logic Controller) platform for distributed industrial automation and management systems that implements the IEC 61499 standard [71]. The standard defines a domain-specific modeling lan-



guage (DSL) for such systems. The platform includes four main components: a runtime environment (RTE), a development environment (IDE), a function block library (LIB), and sample system projects (SYS). The latter includes implementation of Intelligent Electronic Devices (IED) for smart grids which comply with IEC 61499 (model for distributed management systems) and with IEC 61850 (transfer protocol for protection and control technology in electrical switchboards of medium- and high-voltage technology for power supply system automation) [71].

Eclipse Vorto is an open-source tool for creating and managing abstract device descriptions which are neutral in terms of technology (i.e., so-called information models) [72, 73]. Vorto is operated by Bosch and as part of the Bosch Software Innovations (Bosch-SI) Group. It contributes to the standardization of information models for IoT devices. Device manufacturers can create these models with Eclipse Vorto by means of a text-based DSL editor which provides auto-complete, syntax highlighting and content assist (code hinting). The models are abstractions of real devices in terms of status, attributes, and functionalities; they should facilitate the communication between these devices.

Normally, the modeling is done by the device manufacturers. A meta-information model along with Eclipse-based tooling has been developed for designing new information models. Vorto provides a server-based repository for management, release, and reuse as well as collaborative work on these models. Diverse code generators create solutions for various environments such as for Eclipse SmartHome, openHAB, OSGi-DAL, Bosch or Kura. These code generators are provided by the environment providers.

There are numerous other Eclipse IoT projects [74]. Some of these projects include relevant tools, which have been incorporated in Eclipse's Open IoT Stack for Java [75].

Eclipse hawkBit is a *domain-independent back-end framework for rolling out software updates to constrained edge devices as well as more powerful controllers and gateways connected to IP based networking infrastructure* [76]. This industrial provisioning system is built on the Spring Boot framework, which can be adapted to any cloud platform. It also supports flexible deployment management for the rollout of updates on a massive number of devices, clustered as per separate deployment groups including, emergency shutdown, and progress monitoring for the entire rollout and for each group [76].

Papyrus for IoT is a modeling solution based on Eclipse Papyrus and is a part of S3P (Smart, Safe, and Secure Software Development and Execution Platform for IoT) research and development project. Papyrus for IoT enables specification, design, deployment, and monitoring of IoT systems and generates code for Vortex from PrismTech and for IoT-device-operating system from MicroEJ [74, 77].

SensIDL is an open-source development framework that helps sensor developers to specify and implement communication interfaces of intelligent sensors. The specification is done in the same way as Vorto via a DSL [74, 78]. SensIDL uses DSL as standard specification language for defining data provided by sensors, where this description serves as a basis for an automated code generation for the sensors

as well as for the recipients. The generator integrated in SensIDL uses the interface definition as input to generate a semantically enriched interface-specific API [79].

Reactive Blocks is a tool which facilitates the development of software for IoT gateways using graphical modeling and code generation. The generated software is based on Java and OSGi [74, 80].

Node-RED is an open-source tool for graphical modeling and execution of processes in IoT applications—so-called flows. It serves to connect devices, APIs, and online services with each other. The modeled flows are interpreted for runtime. The tool is completely based on Node.js [74, 81].

Virtual Developer is a platform based on Eclipse for automation of programming tasks through code generators. It serves for the development of IoT applications by means of model-driven software development and generates software code for sensors and actors. It also has a Cloud Connector that sends models to servers and receives the generated code [82].

Resin.io is a container-based platform to develop, deploy, and manage code on IoT devices [83]. The platform serves for developing and deploying applications such as environment monitoring, customized retail experiences, or drone deployment on various devices (like Raspberry Pi, Arduino, etc.). Its features include fast iterative development, lightweight and reliable deployment, and management of devices, phased deployments, scheduled updates, etc. [83].

Eclipse Concierge is a lightweight implementation of the OSGi Core specification (a framework for modular software development and deployment), optimized for mobile and embedded devices [61, 84]. Thus, Concierge joins the OSGi framework alongside Equinox, Apache Felix, and Knopflerfish. Concierge has a low footprint; it provides itself as resources to the framework and its internal statuses via a REST (REpresentational State Transfer) interface. Concierge can be integrated with Eclipse SmartHome and OSGi enRoute [61, 84].

The Eclipse Hono project, supported by Bosch and Red Hat, provides a platform for scalable messaging in the field of IoT, where AMQP middleware is connected between devices and back-end services [85, 86]. Devices not supported by AMQP are connected with the protocol adapter, which is responsible for the conversion of AMQP and non-AMQP messages. Moreover, Eclipse Hono collects and processes telemetry data from remote devices centrally by enabling devices to send data to the messaging cloud. Additionally, back-end services can store telemetric data and send commands to the devices.

Eclipse Milo is an implementation of the OPC UA standard, which plays an important role in the automation industry [87]. Therefore, Milo supports IIoT needs, such as access to real-time data, monitoring alarms and events, access to historical data and data modeling.

Californium [88] is a CoAP framework focused on back-end services and IoT devices. It consists of five sub-projects. The Californium-core provides the central framework for protocol implementation in order to develop IoT applications. The sub-project Scandium provides security for Californium and is a pure Java implementation of Datagram Transport Layer Security (DTLS), an encryption protocol [89]. Actinium is the app-server for Californium for implementing IoT mashups.

The sub-project Connector abstracts from the various types of transport which can use CoAP. The sub-project CoAP tools includes tools such as a browser, a command line client, and the CoAPBench for benchmarking customized (CoAP-based) IoT applications [88].

Leshan depends on Californium and presents a complete infrastructure for Java and LWM2M-based IoT solutions. This includes libraries for server and client-side device management, a device management server with web interface as well as a bootstrapping server which is responsible for the security setup of the connected devices [90, 91].

Eclipse Kura is an OSGi-based container for M2M applications which enhances the OSGi and Java standard platforms with APIs and services, which are customized based on the requirements of M2M applications such as I/O access, data services, network configuration and telemetry [62, 92]. Kura is not installed on sensors, but on stronger devices (e.g., Raspberry PI), which function as IoT gateway (receiver/ingestor and distributor). Therefore, Kura undertakes the role of an IoT gateway, i.e., it is responsible for collecting messages from IoT devices and for processing, aggregating, and forwarding these messages. The rule-based routing and mediation engine Apache Camel is set up in Kura, which is responsible for orchestrating the flow of messages. The setup of Camel in Kura is very useful as Camel already includes about 200 OSGi-enabled connectors including JMS, REST, CoAP, AMQP, MQTT, etc.; it also has client-side load balancing. A Camel OSGi Bundle is started from Kura [62, 92]. Kura also contains an Eclipse-based development environment, in which the M2M applications can be developed in emulators and can then be deployed in a target gateway and subsequently transferred on the real-end devices in the field [92].

Eclipse SCADA (also called as Eclipse NeoSCADA) is a modular kit (including extensive IDE) used by developers to implement their own SCADA solutions. The kit includes different protocol adapters (including MQTT, REST, JDBC, Modbus, Siemens S7) and middleware, in order to process data from devices as well as some modules to cover basic functions of a SCADA system (e.g., alarms and events, recording historical data). It also includes user interface components, libraries, and a configuration framework [93, 94].

Eclipse OM2M is an open-source service platform for the interoperability of M2M based on the one M2M standard. OM2M follows a REST-compliant approach with open interfaces in order to facilitate the development of services and applications irrespective of the underlying network. The platform provides a modular architecture above the OSGi layer, which can be enhanced through plug-ins. It supports several protocol connections like HTTP and CoAP. Various proxies interacting smoothly enable seamless communication with manufacturer-specific technologies such as ZigBee [95].

Eclipse Wakaama, like Leshan, is an LWM2M implementation for the client or device side. However, it offers a C-based implementation (and not a Java library), which is portable on POSIX-compliant systems [96].

Temboo is a cloud-based platform with complete software stack for development of IoT applications through code generation. It provides generated code fragments,

which a developer adds in his program code with “Copy & Paste” and processes it further. The code fragments support devices, APIs, databases and online services, where the generated code is dependent on the Temboo SDKs, which are available for different programming languages [74, 97].

Eclipse Ponte is an M2M Bridge Framework for REST development [98]. It serves for the creation of a reusable solution for bridging multiple M2M protocols as per REST. This means that developers formulate a REST-API to read, write and access the history of sensors, actors and other IoT devices. In addition, developers release the MQTT and/or CoAP messages outside using a REST-API. They define an internal API for easy addition of new protocols via plug-ins [98].

### ***1.3.7 IoT Cloud Integration Platforms***

Several cloud providers offer IoT integration platforms to facilitate the collection, processing, and analysis of IoT data using scalable computing. We review the main platforms below.

AWS IoT is the Amazon cloud platform that allows connected things to collaborate easily and securely with cloud applications and other devices. This platform is designed to reliably and securely support billions of connected devices and process trillions of messages, forwarding them to AWS end points or other smart devices. AWS IoT also provides a separate MQTT Message Broker and MQTT Client [99].

Microsoft provides an equivalent cloud platform called Azure IoT, which functions as a hub for reliable and secure bidirectional communication between millions of IoT devices and a solution back end. It also includes an IoT Suite end-to-end implementation of this communication architecture for specific IoT scenarios along with remote monitoring of device status, predictive maintenance and connected factory features for industrial installations [100].

IBM Watson IoT services facilitate easy and efficient application access to IoT devices and data, as well as real-time monitoring and analysis. These also enable the easy building of analytic applications, visualization dashboards, and mobile IoT applications [101].

## **1.4 Conclusions**

In this chapter, we summarized and analyzed the components necessary for an integrated end-to-end IoT solution and highlighted specific IIoT components as appropriate. Our analysis goes beyond existing studies, including our own previous work, by specifically focusing on all IoT solution components—rather than just subsets—relating to both solution development and operations. To our knowledge, this is the first attempt to provide such an examination of the state of the art. By highlighting the advantages and disadvantages of choosing different IoT components, we hope

that our analysis is helpful to IoT practitioners designing IoT systems with diverse requirements. We also hope that this analysis can help students as well who are interested in learning about IoT, as well as researchers interested in understanding the current IoT landscape and its limitations, to support them in the creation of new standards, tools, and frameworks.

**Acknowledgements** The authors would like to thank Capgemini for supporting the editing of the present contribution. The authors would also like to thank all the anonymous reviewers who made many valuable suggestions for improving the text.

## References

1. Ashton K (2011) That ‘internet of things’ thing. *RFID J* 22
2. Columbus L (2018) A roundup of 2018 enterprise Internet of things forecasts and market estimates. *Enterprise CIO*
3. Gold J (2018) What is the industrial IoT? [and why the stakes are so high]. *Network World*
4. Hofmann E, Rüscher M (2017) Industry 4.0 and the current status as well as future prospects on logistics. *Comput Ind* 89:23–34
5. Columbus L (2018) 10 charts that will challenge your perspective of IoT’s growth. *Forbes*
6. Papert M, Pflaum A (2017) Development of an ecosystem model for the realization of internet of things (IoT) services in supply chain management. *Electron Markets* 27:175–189
7. Prasse C, Nettstraeter A, ten Hompel M (2014) How IoT will change the design and operation of logistics systems. In: *Proceedings of IEEE international conference on the internet of things (IOT)*. Cambridge, MA, USA
8. Guerrero-ibanez JA, Zeadally S, Contreras-Castillo J (2015) Integration challenges of intelligent transportation systems with connected vehicle cloud computing, and internet of things technologies. *IEEE Wireless Commun* 22:122–128
9. He W, Yan G, Xu LD (2014) Developing vehicular data cloud services in the IoT environment. *IEEE Trans Industr Inf* 10:1587–1595
10. Iansiti M, Lakhani KR (2014) Digital ubiquity: how connections, sensors, and data are revolutionizing business. *Harvard Bus Rev* 92:91–99
11. Chen S, Xu H, Liu D, Hu B, Wang H (2014) A vision of IoT: applications challenges, and opportunities with China perspective. *IEEE Internet of things J* 4:349–359
12. Kim J, Yun J, Choi SC, Seed DN, Lu G, Bauer M, Al-Hezmi A, Campowsky K, Song J (2016) Standard-based IoT platforms interworking: implementation, experiences, and lessons learned. *IEEE Commun Mag* 54:48–54
13. Chen C, Helal S (2008) Sifting through the jungle of sensor standards. *IEEE Pervasive Comput* 7:84–88
14. Chircu AM, Sultanow E, Sözer L (2017) A reference architecture for digitalization in the pharmaceutical industry. In: Eibl M, Gaedke M (eds) *Workshops der INFORMATIK 2017. Lecture notes in informatics (LNI)*. Gesellschaft für Informatik, Bonn
15. Sultanow E, Chircu AM, Schroeder K, Kern S (2018) A reference architecture for pharma, healthcare & life sciences: a framework for using digital technology. In: Czarnecki C et al (eds) *Workshops der INFORMATIK 2018. Lecture Notes in Informatics (LNI)*. Gesellschaft für Informatik, Bonn
16. Sultanow E, Chircu AM (2018) Bringing clarity to the java IoT jungle. *Issues Inform Syst* 19(4):26–34
17. Boyes H, Hallaq B, Cunningham J, Watson T (2018) The industrial Internet of things (IIoT): an analysis framework. *Comput Ind* 101:1–12

18. Lasi H, Fettke P, Kemper HG, Feld T, Hoffman M (2014) Industry 4.0, business & information. *Syst Eng* 6:239–242
19. Drath R Horch A (2014) Industrie 4.0: hit or hype? [industry forum]. *IEEE Industrial Electron Mag* 8(2):56–58
20. Lu Y (2017) Industry 4.0: a survey on technologies, applications and open research issues. *J Industrial Inf Integr* 6:1–10
21. Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W (2017) A survey on internet of things: architecture enabling technologies, security and privacy, and applications. *IEEE Internet of things J* 4(5):1125–1142
22. Xu LD, He W, Li S (2014) Internet of things in industries: a survey. *IEEE Trans Industr Inf* 10(4):2233–2243
23. Pang Z, Zheng L, Tian J, Kao-Walter S, Dubrova E, Chen Q (2015) Design of a terminal solution for integration of in-home health care devices and services towards the internet-of-things. *Enterp Inf Syst* 9(1):86–116
24. Ramirez ARG, González-Carrasco I, Jasper GH, Lopez AL, Lopez-Cuadrado JL, García-Crespo A (2017) Towards human smart cities: internet of things for sensory impaired individuals. *Computing* 99(1):107–126
25. Dhariwal K, Mehta A (2017) Architecture and plan of smart hospital based on internet of things (IOT). *Int Res J Eng Technol* 4(4):1976–1980
26. Zhang Y, Zhang G, Wang J, Sun S, Si S, Yang T (2015) Real-time information capturing and integration framework of the internet of manufacturing things. *Int J Comput Integr Manuf* 28(8):811–822
27. Zancul EDS, Takey SM, Barquet APB, Kuwabara LH, Cauchick Miguel PA, Rozenfeld H (2016) Business process support for IoT based product-service systems (PSS). *Bus Process Manage J* 22(2):305–323
28. Wang K, Wang Y, Sun Y, Guo S, Wu J (2016) Green industrial internet of things architecture: an energy-efficient perspective. *IEEE Commun Mag* 54(12):48–54
29. Liu X, Zhao M, Li S, Zhang F, Trappe W (2017) A security framework for the internet of things in the future internet architecture. *Future Internet* 9(3):1–28
30. Yang Y, Wu L, Yin G, Li L, Zhao H (2017) A survey on security and privacy issues in internet-of-things. *IEEE Internet of things J* 4(5):1250–1258
31. Lin SW, Murphy B, Clauer E, Loewen U, Neubert R, Bachmann G, Pai M, Hankel M (2017) Architecture alignment and interoperability: an industrial internet consortium and platform industries 4.0 joint whitepaper. Industrial Internet Consortium, 5 Dec 2017, [https://www.iiconsortium.org/pdf/JTG2\\_Whitepaper\\_final\\_20171205.pdf](https://www.iiconsortium.org/pdf/JTG2_Whitepaper_final_20171205.pdf). Accessed 25 Jan 2019
32. IBM (2018) Internet of things for Insights from Connected Devices, <https://www.ibm.com/cloud/garage/architectures/iotArchitecture>. Accessed 25 Jan 2019
33. Object Management Group (2018) DDS, <https://www.omgwiki.org/dds/>. Accessed 25 Jan 2019
34. Open Connectivity Foundation (2018) Solving The IoT Standards Gap, <https://openconnectivity.org/>. Accessed 25 Jan 2019
35. Internet of things Consortium (2018) Internet of things Consortium (IoTC), <https://www.iotone.com/organization/internet-of-things-consortium-iotc/o182>. Accessed 25 Jan 2019
36. Eclipse Foundation (2018) Open Source for IoT, <https://iot.eclipse.org/>. Accessed 25 Jan 2019
37. Singh K, Kapoor D (2017) Create your own internet of things: a survey of IoT platforms. *IEEE Consum Electron Mag* 6:57–68
38. CNXSoft (2016) How to use Sonoff POW ESP8266 WiFi power switch with MQTT and Thing Speak, 11 Dec 2016, <https://www.cnx-software.com/2016/12/11/how-to-use-sonoff-pow-esp8266-wifi-power-switch-with-mqtt-and-thingspeak/>. 17 Nov 2018
39. Gold J (2016) Sigfox and LoRa are the WiMax of IoT. *Computerworld*, 12 Sep 2016, <https://www.computerworld.com/article/3117795/cloud-computing/sigfox-and-lora-are-the-wimax-of-iot.html>. Accessed 17 Nov 2018
40. Deutsche Telekom (2017) Narrowband IoT: the game changer for the internet of things. 1 Oct 2017, [http://m2m.telekom.com/fileadmin/media/Whitepaper\\_NarrowBand\\_IoT\\_-\\_The\\_Game\\_Changer\\_for\\_the\\_Internet\\_of\\_Things\\_-\\_1.10.2017.pdf](http://m2m.telekom.com/fileadmin/media/Whitepaper_NarrowBand_IoT_-_The_Game_Changer_for_the_Internet_of_Things_-_1.10.2017.pdf). Accessed 17 Nov 2018

41. Hwang Y (2018) Cellular IoT explained—NB-IoT versus, LTE-M versus, 5G and More, <https://www.leverage.com/blogpost/cellular-iot-explained-nb-iot-vs-lte-m>. Accessed 29 Feb 2018
42. Mehboob U, Zaib Q, Usama C (2016) Survey of IoT communication protocols techniques, applications, and issues, <http://xflowresearch.com/wp-content/uploads/2016/02/Survey-of-IoT-Communication-Protocols.pdf>. Accessed 25 Feb 2018
43. Viswanathan P (2018) 4G mobile networks: the pros and the cons. 12 Nov 2018, <https://www.lifewire.com/4g-mobile-networks-pros-and-the-cons-2373260>. Accessed 17 Nov 2018
44. Hwang Y (2016) Cellular IoT explained—NB-IoT versus, LTE-M versus, 5G and More, 30 Dec 2016, <https://www.leverage.com/blogpost/cellular-iot-explained-nb-iot-vs-lte-m>. Accessed 25 Feb 2018
45. Matten L (2016) NB-IoT: pros and cons of the new LPWA radio technology, 11 Oct 2016, [https://de.slideshare.net/M2M\\_Alliance/nbiot-pros-and-cons-of-the-new-lpwa-radio-technology](https://de.slideshare.net/M2M_Alliance/nbiot-pros-and-cons-of-the-new-lpwa-radio-technology). Accessed 25 Feb 2018
46. Obermaier D (2015) IoT-Protokollsdchungel—Ein Wegweiser, 17 Nov 2015, <https://www.informatik-aktuell.de/betrieb/netzwerke/iot-protokollsdchungel-ein-wegweiser.html>. Accessed 17 Nov 2018
47. Stanford-Clark A, Truong HL (2013) MQTT for sensor networks (MQTT-SN) protocol specification Version 1.2. International Business Machines Corporation (IBM), 14 Nov 2013, [http://mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN\\_spec\\_v1.2.pdf](http://mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf)
48. Diwan M, D'Souza M (2017) A framework for modeling and verifying IoT communication protocols. In: Larsen K, Sokolsky O, and Wang J (eds) Dependable software engineering. Theories, tools, and applications. SETTA 2017. Lecture Notes in Computer Science. Springer, Cham
49. Prado J (2016) OMA lightweight M2M resource model, [https://www.iab.org/wp-content/IAB-uploads/2016/03/OMA\\_LightweighM2M\\_Resource\\_Model\\_Summary.pdf](https://www.iab.org/wp-content/IAB-uploads/2016/03/OMA_LightweighM2M_Resource_Model_Summary.pdf). Accessed 25 Feb 2018
50. PrismTech (2017) Messaging technologies for the industrial internet and the internet of things whitepaper. 12 May 2017, <http://www.prismtech.com/sites/default/files/documents/Messaging-Whitepaper-051217.pdf>. Accessed 25 Feb 2018
51. Melo M (2018) CoAP and MQTT-SN: explained, <https://www.sine-wave.com/blog/mqtt-sn-and-coap#.WpLrqExFzvM>. Accessed 25 Feb 2018
52. Semle A (2015) IIoT protocols to watch, 26 Oct 2015, <https://www.automation.com/library/white-papers/iiot-protocols-to-watch>. Accessed 25 Feb 2018
53. Kowalke M (2015) The pros and cons of the major IoT communications protocols, 20 Aug 2015, <http://www.realtimecommunicationsworld.com/topics/realtimecommunicationsworld/articles/408622-pros-cons-the-major-iiot-communications-protocols.htm>. Accessed 25 Feb 2018
54. GitHub (2018) XMPP-IoT, <https://github.com/joachimlindborg/XMPP-IoT>. Accessed 17 Nov 2018
55. Rahman RA, Babar S (2017) Security analysis of IoT protocols: a focus in CoAP. In: Proceedings of the 3rd MEC international conference on big data and smart city (ICBDSC), Muscat, Oman, March 2016, pp 1–7
56. B&R Industrial Automation GmbH (2018) TSN and Pub/Sub: real-time capability for OPC UA, <https://www.br-automation.com/en/technologies/opc-ua/tsn-and-pubsub/>. Accessed 17 Nov 2018
57. Naik N (2017) Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In: Proceedings IEEE international systems engineering symposium (ISSE), Vienna, Austria, Oct 2017, 1–7
58. Feldmann M (2016) A new cluster for HiveMQ 3.1, 7 Mar 2016, <https://jaxenter.de/ein-neuer-cluster-fuer-hivemq-3-1-36033>. Accessed 17 Nov 2018
59. Eclipse Foundation (2018) Open Source for IoT, <https://iot.eclipse.org/>. Accessed 17 Nov 2018

60. Eclipse Foundation (2018) Moquette MQTT, <https://projects.eclipse.org/projects/iot.moquette>. Accessed 17 Nov 2018
61. Eclipse Foundation (2018) Eclipse Concierge, <https://projects.eclipse.org/projects/rt.concierge>. Accessed 17 Nov 2018
62. Eclipse Foundation (2018) Kura, <https://www.eclipse.org/kura/>. Accessed 17 Nov 2018
63. RabbitMQ (2018) MQTT Adapter, <https://www.rabbitmq.com/mqtt.html>. Accessed 17 Nov 2018
64. Eclipse Foundation (2018) Eclipse Paho, <https://www.eclipse.org/paho/>. Accessed 17 Nov 2018
65. Artmann M (2017) OpenHAB 2.1—new level for smart-home-management, 9 Sep 2017, <https://www.homeandsmart.de/openhab-2-smart-home-software-open-source>. Accessed 17 Nov 2018
66. Mann M, Götz C (2015) Smart home in action with openHAB and MQTT. Eclipse Magazin 2
67. Menge R (2017) Smart home: openHAB 2.1 can access Eclipse IoT Market, 28 Jun 2017, <https://www.heise.de/developer/meldung/Smart-Home-openHAB-2-1-kann-auf-Eclipse-IoT-Market-zugreifen-3757723.html>. Accessed 17 Nov 2018
68. Schmidt J (2014), Eclipse smarthome is designed to prevent fragmentation in the smart home area, 17 Jun 2014, <https://www.heise.de/developer/meldung/Eclipse-SmartHome-soll-Fragmentierung-im-Smart-Home-Bereich-verhindern-2225118.html>. Accessed 17 Nov 2018
69. Eclipse Foundation (2018) Edje, <https://projects.eclipse.org/proposals/edje>. Accessed 17 Nov 2018
70. Eclipse Foundation (2018) Eclipse Ditto, <https://projects.eclipse.org/proposals/eclipse-ditto>. Accessed 17 Nov 2018
71. Eclipse Foundation (2018) Eclipse 4diac, <https://www.eclipse.org/4diac/>. Accessed 17 Nov 2018
72. Eclipse Foundation (2018) Eclipse Vorto, <https://www.eclipse.org/vorto/>. Accessed 17 Nov 2018
73. Scheib J, Laverman J, Wagner M, Weinmann O (2016) Eclipse Vorto interoperability for Internet of things. Eclipse Magazin 3
74. Munzert M (2016) Industrial IoT solutions with eclipse IoT and model-driven development, 21 May 2016, <http://www.informatik-aktuell.de/entwicklung/methoden/industrielle-iiot-loesungen-mit-eclipse-iiot-und-mdsd.html>. Accessed 17 Nov 2018
75. Eclipse Foundation (2018) Open IoT stack for java, <https://iiot.eclipse.org/java/open-iiot-stack-for-java.html>. Accessed 17 Nov 2018
76. Eclipse Foundation (2018) hawkBit, <https://projects.eclipse.org/proposals/hawkbit>. Accessed 17 Nov 2018
77. Dhoubi S, Cucuru A, Le Fèvre F, Li S, Maggi B, Paez I (2016) Papyrus for IoT—a modeling solution for IoT. In: Proceedings l’Internet des Objets (IDO: Nouveaux Défis de l’Internet des Objets: Interaction Homme-Machine et Facteurs Humains. Paris, France
78. SensIDL (2018) A generic framework for implementing sensor communication interfaces, <http://sensidl-project.github.io/SensIDL/>. Accessed 17 Nov 2018
79. Groenda H, Rathfelder C, Taspolatoglu E (2015) SensIDL: Ein Werkzeug zur Vereinfachung der Schnittstellenimplementierung intelligenter Sensoren, [https://www.sigs-datacom.de/uploads/tx\\_dmjournals/Groenda\\_Rathfelder\\_Taspolatoglu\\_OTs\\_IoT\\_2015.pdf](https://www.sigs-datacom.de/uploads/tx_dmjournals/Groenda_Rathfelder_Taspolatoglu_OTs_IoT_2015.pdf). Accessed 17 Nov 2018
80. BitReactive (2018) Reactive Blocks, <http://www.bitreactive.com/reactive-blocks>. Accessed 17 Nov 2018
81. Node-RED (2018) Node-RED Flow-based programming for the Internet of things, <https://nodered.org>. Accessed 17 Nov 2018
82. Generative Software (2018) Virtual Developer, <https://www.virtual-developer.com>. Accessed 17 Nov 2018
83. Resin.io (2018) Resin.io, <https://resin.io>. Accessed 17 Feb 2018



84. Hiller J (2015) Eclipse concierge—fit for IoT? OSGi for Embedded Systems in the Internet of things. Eclipse Magazine, USA, p 2
85. Eclipse Foundation (2018) Eclipse Hono, <https://projects.eclipse.org/projects/iot.hono>. Accessed 17 Nov 2018
86. Mohilo D (2016) Eclipse Weekly: Neon M7, Andmore-Update und das neue Projekt Eclipse Hono, 11 May 2016, <https://jaxenter.de/eclipse-weekly-neon-m7-andmore-update-und-das-neue-projekt-eclipse-hono-40055>. Accessed 17 Nov 2018
87. Eclipse Foundation (2018) Eclipse Milo, <https://projects.eclipse.org/projects/iot.milo>. Accessed 17 Nov 2018
88. Eclipse Foundation (2018) CoAP in Java, <https://www.eclipse.org/californium/>. Accessed 17 Nov 2018
89. Caposese A, Cervo V, De Cicco G, Petrioli C (2015) Security as a CoAP resource: an optimized DTLS implementation for the IoT. In: Proceedings of IEEE international conference on communications (ICC), London, UK
90. Schlosser H (2014) New IoT Project Proposed: Eclipse Leshan, 12 Sep 2014, <https://jaxenter.de/neues-iot-projekt-vorgeschlagen-eclipse-leshan-639>. Accessed 17 Nov 2018
91. Eclipse Foundation (2018) Leshan, <http://www.eclipse.org/leshan/>. Accessed 17 Nov 2018
92. Schlosser H (2013) Eclipse Kura: Internet of things on OSGi, 25 Jul 2013, <https://jaxenter.de/eclipse-kura-das-internet-der-dinge-auf-osgi-2889>. Accessed 17 Nov 2018
93. Rose J, Reimann J (2015) Tutorial for IoT project for Eclipse: Eclipse SCADA tutorial, 3 Mar 2015, <https://jaxenter.de/eclipse-scada-tutorial-teil-1-15166>. Accessed 17 Nov 2018
94. Eclipse Foundation (2018) Eclipse NeoSCADA, <https://eclipse.org/eclipse-scada/>. Accessed 17 Nov 2018
95. Eclipse Foundation (2018) Eclipse OM2M, <https://projects.eclipse.org/projects/technology.om2m>. Accessed 17 Nov 2018
96. Eclipse Foundation (2018) Wakaama, <https://eclipse.org/wakaama/>. Accessed 17 Nov 2018
97. Temboo (2018) Tools for digital transformation, <https://temboo.com/>. Accessed 17 Nov 2018
98. Eclipse Foundation (2018) Eclipse Ponte. <https://projects.eclipse.org/projects/technology.ponte>. Accessed 17 Nov 2018
99. Amazon (2018) AWS IoT <https://aws.amazon.com/iot>. Accessed 17 Nov 2018
100. Microsoft (2018) Overview of the Azure IoT *Hub Service*, <https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-what-is-iot-hub#iot-device-connectivity-challenges>. Accessed 19 Dec 2018
101. IBM (2018) Watson Internet of things, <https://www.ibm.com/internet-of-things>. Accessed 19 Dec 2018

## Chapter 2

# Industrial Internet of Things (IIoT): Principles, Processes and Protocols



Somayya Madakam and Takahiro Uchiya

**Abstract** The Industrial Internet of Things (IIoT) is a paradigm shift, primarily in the domain of manufacturing industry. The concept is highly attractive for a majority of the industrial sectors due to better operational efficiency capabilities in the production process, smart objects identification mechanisms by embeddedness technologies, intelligent automation abilities and around the clock monitoring abilities. Importantly, it reduces workforce intervention in risky industrial environments. Some of the best practicing places and activities for the IIoT employment are factory shop floors, materials handling, assembly lines, production processes, finalising goods, and other inbound and outbound logistical tasks. The basis for the IIoT phenomenon growth is the Internet of Things (IoT) technologies, which have currently been ensuring efficient work execution in many spheres, industrial as well as commercial and social. This chapter provides a discussion on IIoT concepts and definitions, on business drivers behind the growth of this technology, and the evolution process of this phenomenon. This contribution also discusses the fundamental underlying principles, related technologies, deployment approaches in different areas and associated frameworks. The chapter also explore Japanese Industry-specific case studies, where the industries have already been employing the IIoT-related practices. These include Zenitaka Corporation, Tsuchiya-Gousei, Toyota and Hitachi. This book chapter provides a broader overview in crystal clear and sets the background for the rest of the chapters in this book.

**Keywords** Industrial internet of things · IIoT · Internet of things · IoT · Industry 4.0 · Smart factory · Operational efficiency · M2M · Japan

---

S. Madakam (✉)  
FORE School of Management, New Delhi, India  
e-mail: [somayya@fsm.ac.in](mailto:somayya@fsm.ac.in)

T. Uchiya  
Nagoya Institute of Technology, Nagoya, Japan  
e-mail: [t-uchiya@nitech.ac.jp](mailto:t-uchiya@nitech.ac.jp)

## 2.1 Introduction

Technologies play an important role in our day-to-day life, as well as for business, government agencies and industries such as entertainment, tourism, aviation, transportation, healthcare and manufacturing, especially from 1960 onwards. Most of the Industrial Internet of Things (IIoT) technologies are helping in many ways in terms of identifications of objects, monitoring events, automation and monitoring of risky processes and environments, and in general, making available the services for people around the clock and securing people and things from anthropogenic and natural calamities. Under the realm of the IIoT technologies, the IIoT, also known as 'Industry 4.0' (or I4.0) is now seen in the context of industrial transformation across the globe. Smart manufacturing is the dramatically intensified and pervasive application of networked information-based technologies; so are the supply chain and logistics enterprises [1].

The current fourth industrial revolution (Industry 4.0) is gradually manifesting itself in all global industrial firms. It is based on the Internet of Things paradigm and service-oriented concepts relating to manufacturing and other industrial sectors, which has led to vertically and horizontally integrated production systems [2]. The underlying understanding is that smart machines with embedded IoT technologies are better than manually operated processes at correctly capturing, analysing, storing and communication of data from/to the other interconnected objects in real time and around the clock. This phenomenon is gradually taking hold in all industry sectors including oil and gas, energy production, coal mining, chemical plants, manufacturing units, pharmaceutical companies, logistics processes, shipping handling and aviation business, etc.

Manufacturers and industrialists in every sector have a significant opportunity at hand, to not only monitor but also automate many of the complex processes involved in their industries. While there have been systems that can track the progress of manufacturing and production, the Industrial IoT provides far more intricate control to the managers. Under the umbrella of IIoT, many technologies are getting embedded in the factory machines, materials and methods, including machine learning, artificial intelligence (AI), machine-to-machine (M2M) communication, distributed computing, cloud computing, edge computing and data analytics. Hence, the IIoT technology is an amalgamation of different technologies like machine learning, big data, sensor data, M2M communication and automation, which have existed in the industrial backdrop for many years.

A typical IIoT system consists of intelligent systems like software applications, microcontrollers, sensors and system security mechanisms. Government policies on Industry 4.0, Smart Factories, Make In India, Make In China 2025, Smart Cities and Japan's Industrial Value Chain Initiative Forum along with enlightened support for green initiatives, rising energy and crude oil prices, favourable FDI, regulatory bodies, etc. have propelled the IIoT evolution to its current favourable state.

With this background, this book chapter aims to discuss, in some detail, the IIoT principles, processes and protocols.

The next sections discuss in detail the concepts of Industrial Internet of Things and the evolution in automation. In addition, this book chapter explores certain IIoT-based test cases in Japan.

## 2.2 Industrial Internet of Things (IIoT)

The Industrial Internet of Things, or IIoT, is the use of IoT technologies to enhance manufacturing and industrial processes. The IIoT (also known as the Industrial Internet, Industry 4.0 and Smart Factory) incorporates machine learning, deep learning and big data technologies to harness the sensor data, machine-to-machine (M2M) communication and automation technologies that have existed in industrial settings for several years. This concept includes all the physical materials of the factories, with the aim to enhance the operational efficiency of processes.

In recent years, there have been great advances in the IIoT and related domains, such as industrial wireless networks (IWNs), big data, and cloud/fog computing, etc. These emerging technologies bring greater opportunities for promoting industrial upgrades and allowing the introduction of the fourth industrial revolution, namely, Industry 4.0 [3]. Industrial Internet helps to develop connected enterprises by merging the information and operational sectors of the industry. This improves visibility, boosts operational efficiency, increases productivity and reduces the complexity of process in the industry. Hence, the Industrial IoT helps with transformative manufacturing and production strategies that further help to improve quality, productivity and safety of the workforce. For instance, a machine can give advance notification to the owners or operators about an imminent breakdown or onset of an unacceptable environment (e.g., temperature rising beyond a critical limit). In other scenarios, smart glasses can allow field technicians to work hands-free while remote supervisors walk them through solutions. Intelligent factory floors can be connected to a cloud platform to obtain the status of raw material progress in real time. Such examples reflect how a manufacturing unit can be transformed with the aid of IIoT.

A typical IIoT system consists of intelligent system applications, micro controllers, wireless sensors, and smart security mechanisms, plus fully connected high speed data communication infrastructure including cloud computing and edge computing provision, etc. Moreover, data analytics are used to support business intelligence and corporate decision-making processes, not to forget the most critical human element aspect. The benefits that Industrial Internet of Things (IIoT) promises include enhanced safety, better reliability, smart metering, inventory management, equipment tracking and smart facilities.

A research study by Genpact [4] concludes that almost 81% of global organisations believe that successful adoption of Industrial Internet of Things is critical to future success—even more so for high-tech and large enterprises. It is well recognised that this latest wave of technological change will bring unprecedented opportunities, along with new risks, to business organisations and the society at large. It will combine the global reach of the Internet with a new ability to directly control the physical

world, including the machines, factories and infrastructure that define the modern industrial landscape.

However, like the Internet was in the late 1990s, the Industrial Internet is currently in its early stages. Many important questions remain unanswered, including how it will impact existing value chains, business models, workforces, and what business actions and government leaders need to take now to ensure long-term success. While the IoT affects among other sections such as transportation, healthcare and smart homes, IIoT refers in particular to industrial processes and environments [4].

## 2.3 The Driving Factors

Today, the manufacturing and production environment for Industry 4.0 is mostly characterised by fast-changing processes, short development periods, abrupt technological evolutions and a growing necessity for individual demand and customised products. Consequently, significant changes are occurring in firms, not only for the physical plants but also for future technological manufacturing skills and competencies required for driving Industry 4.0 forward [5]. Industrial and IP-enabled low-power wireless networking technologies are emerging, resulting in the further advancement of IIoT [6]. In general, the growth of the IoT is making an emphatic impact on homes and industries.

While the IoT influences transportation, healthcare and smart homes, the IIoT refers in particular to industrial environments. IIoT is a new industrial ecosystem that combines intelligent and autonomous machines, advanced predictive analytics, and machine–human collaboration to improve productivity, efficiency and reliability. It is bringing about a world where smart, connected embedded systems and products operate as part of larger systems. The IIoT is already revolutionising manufacturing by enabling the acquisition and accessibility of far greater amounts of data, at far greater speeds, and far more efficiently than before. Some innovative companies have started to implement IIoT by leveraging intelligent and connected devices in their factories. The prime driving forces of IIoT across the globe can be considered and discussed as follows:

- The driving philosophy behind Industrial Internet of Things is that smart machines are better than humans at accurately and consistently capturing and communicating real-time data. This data enables companies to pick up on inefficiencies and problems much sooner, and thus saving time and money and supporting business intelligence efforts.
- Technology of smart sensors, robotics and automation, augmented/virtual reality, big data analytics, cloud integration, software applications, mobile, low-power hardware devices and scalability of IPv6-3.4x 10<sup>38</sup> IP address, etc. are also the major drivers for the industrial internet.

- The edge that IIoT gives to enterprises over their competitors helps them achieve better customer satisfaction and retention through value addition that IIoT inherently provides.
- Government policies on Industry 4.0, Smart Factories, Make In India, Smart Cities, Make In China 2025, and Japan's Industrial Value Chain Initiative Forum, supporting the green initiatives, rising energy and crude oil prices, and favourable FDI, etc. are all helping to fuel the IIoT evolution.

Thus, there are several factors that contribute to the growing global popularity for Industrial Internet of Things practices. Clearly, IIoT is not limited to one particular country or a particular industry type, as it is popularised across healthcare, pharmaceutical, transportation, R&D, aviation, mining and many more sectors.

## 2.4 Evolution of IIoT

The IIoT may be considered as the twenty-first century's industrial revolution, hence the term 'Industry 4.0'. Phenomenally, Industry 4.0 is rapidly changing firms' management, organisational systems and competencies, even if they are becoming more complex than in the past [5]. However, the IIoT phenomenon is growing fast. Indeed, the advent of IIoT-related technologies can be traced to the steam engines and moving to mass production, and electronics embeddedness in the manufacturing process, and then to the popularity of the Internet. It is indeed a long journey for today's Industrial IoT since the Industry 1.0 of 1776. The following lists present a brief summary of the development of the IIoT paradigm.

- **Industry 1.0 (1784)**—This was the first phase of industrialisation. However, the invention of steam engines kick-started the Industry 1.0 phase. The manufacturing was purely labour-oriented and tiresome at this stage.
- **Industry 2.0 (1870)**—The first assembly line production was introduced during this phase of evolution. This stage was a big relief for the workers as their labour was reduced to some extent. Henry Ford introduced the assembly line to automate processes in car manufacturing, and elsewhere as well, to improve the productivity using conveyor belt mechanism.
- **Industry 3.0 (1969)**—The third phase of the industrial revolution started in around 1969. It involved the advancement of electronic technology and industrial robotics. Miniaturisation of electronic circuit boards through programmable logic controllers and development of industrial robotics simplified, automated and increased the production. However, in Industry 3.0, the operations remained isolated and independent within the entire enterprise.
- **Industry 4.0 (2010)**—This evolution started around 2010, but gained popularity only from around 2016. The vision of connected enterprise through the interconnection of industrial assets through the Internet was fulfilled with the introduction of Industry 4.0. The interconnected smart devices communicate with each other, and cloud paradigm and data analytics created valuable business insights. IIoT

brought the advantages of asset optimisation, production integration, smart monitoring, remote diagnosis, intelligent decision-making and most importantly, the predictive and autonomous maintenance. Industry 4.0 thus presented a paradigm shift from automated manufacturing towards intelligent manufacturing. Unlike the previous industrial revolutions, the current fourth revolution aims to be more decentralised, automated and controlled via interdependence [9].

In November 2016, the International Society of Automation (ISA), Process Control and Safety Forum (PCS) in Houston Texas, and ISA's Communication division convened a panel to focus and discuss on the Industrial Internet of Things. In the panel, experienced industrial and control engineers shared their views, concerns and reservations with IIoT [7], in spite of the fact that the Industry 4.0 offers enormous and radically new market approach and segmentation [8]. Their deliberations and recommendations helped move the IIoT agenda further.

## **2.5 IoT Applications in the Industry**

The Industrial IoT phenomenon is a magic wand for any national economy. The IIoT covers many industrial applications. It yields plenty of opportunities in automation, manufacturing, transportation, pharmaceutical, mining and chemical industry, just to name a few. Potgieter [10] states that the IIoT ecosystem comprises data generating equipment like sensors, actuators and gateways, which sit atop platforms that integrate and feed the required data to applications through dashboards or other reports, where decisions are made and controlled at the central server [10]. Another study by Dujovne et al. [6] reported that the industrial and IP-enabled low-power wireless networking technologies have converged, resulting in today's IIoT [11]. A number of industry-wide applications are now discussed in the following subsections.

### **2.5.1 Manufacturing**

Manufacturing has the largest IIoT market. It is a major industry, from the perspective of IoT depending on software, hardware, network connectivity and services. Manufacturing is among the industrial sectors that is directly impacted by the disruption from the Industrial IoT. A smart production unit may consist of a large interconnected industrial system of materials, parts, machines, tools, inventory and logistics that can relay data and communicate with each other. IIoT connectivity drives the convergence of operational technology like robots, conveyor belts, smart metres and generators. In the manufacturing sector, intelligent sensors, distributed control and secure software are the crucial elements. Forward-thinking manufacturers connect their products to IIoT. They will position themselves as future leaders, while those that fail to act will risk being left behind. In manufacturing specifically,

IIoT holds great potential for quality control, sustainable and green practices, supply chain traceability and overall supply chain efficiency. In an industrial setting, IIoT is key to processes such as predictive maintenance (PdM), enhanced field service, energy management and asset tracking. The IIoT can be regarded as an industrial machine connected to the enterprise cloud storage area for data storage as well as data retrieval and processing [12].

### ***2.5.2 Transportation***

The Industrial IoT includes a network of smart power, manufacturing, medical and transportation [13]. The transportation domain represents the second largest IIoT market from the perspective of expenditure on IoT applications. Today's transportation infrastructure is stressed to the breaking point. Many cities have begun smart transportation initiatives to optimise their public transportation routes, create safer roads, reduce infrastructure costs and alleviate traffic congestion. Especially, the airlines, rail companies and public transit agencies can aggregate enormous quantities of data to optimise operations. Smart cards, online reservations and in-vehicle Google mapping are some of the industry-specific applications to transportation. IIoT may be considered an amalgamation of 'Intelligent Enterprises' and 'Intelligent Machines' to manage the vehicular machines such as cars and trucks [14].

### ***2.5.3 Energy and Utilities***

Increasing cost and demand for energy have led many organisations to find smarter ways for monitoring, controlling and saving energy [15]. Hence, the oil and gas, smart grid and other related developments in the energy and utilities sector also forms a central part of the IIoT vision. According to the data from International Data Corporation (IDC), utilities represent the third most attractive industry, on the basis of expenditure in IoT, having reached a total of \$69 billion in 2016. One area of investment that emerges as especially important is the smart grids for electricity and gas, which accounted for a huge \$57.8 billion in 2016. Many industries are attempting to use better and smarter sensor-based management systems with the help of the Industrial IoT vision.

### ***2.5.4 Healthcare***

IoT provides new opportunities to improve healthcare systems. Having been powered by the IoT's ubiquitous identification, sensing and communication capacities, all objects in the healthcare systems including people, equipment, medicine, etc.



can be tracked and monitored constantly. Enabled by its global connectivity, all the healthcare-related information in logistics, diagnosis, therapy, recovery, medication, management, finance and even daily activities can be collected, managed and shared efficiently. For example, a patient's heart rate data can be collected by sensors at frequent intervals and then sent to the healthcare practitioners, e.g. doctors. By using personal computing devices like a laptop, mobile phone, tablet, and computer internet access, the IoT-based healthcare services can be mobilised and personalised to provide better care. The widespread mobile Internet service has expedited the development of IoT-powered in-home healthcare services. However, security and privacy concerns are two major challenges.

Health IIoT is a combination of communication technologies, interconnected apps, smart objects and people that would function together as one smart system to monitor, track and store patients' healthcare information for ongoing care [16]. Several healthcare-related IIoT applications are expected to widely utilise the evolving 5G communication technology. This 5G-inspired Industrial Internet of Things paradigm in healthcare enables users to interact with various types of sensors via secure Wireless Medical Sensor Networks [17].

## 2.6 IIoT Use Cases in Japanese Industry

Japan is well-known for her industries, firms and manufacturing units across Asia as well as the globe. Some of the big organisations that embraced the IIoT paradigm include: Toyota Motors, The LollipopRoad, Mitsubishi UFJ Financial, Luxatic, Sumitomo Mitsui Financial, The Business Times, Nippon Telegraph & Tel, Wiki-media Commons, Honda Motors, Sakura, Softbank, technobuffalo, Mizuho Financial, Japan Times and Nissan Motors.

Interestingly, Japan is a very small country in terms of geographical area with a low population; however, it is a fabulous manufacturing hub for automobile, banking, telecom, media, technological, service sector, agricultural and much else. Their culture and customs are unique from the rest of the world.

Recently, the Japan government has made concentrated attempts to promote research and development in the three key research areas: IoT, big data analytics and AI. Refer to the white paper 2018 [18] developed by the Japan Ministry of Internal Affairs and Communication. It suggests that, in order to realise productivity improvement and rich secure living in Japanese society amid the fierce competition in the era of IoT, BDA and AI, the technology Strategy Committee, Information Communication Technology Subcommittee of Information and Communications Council has already compiled the third interim report in July 2017. The report points to the Next Generation AI Commercialisation Strategy and the Next Generation AI with ICT Adaptability Strategy to ensure commercialisation for utilisation of super mass data that will further enhance the commercialisation. In order to study medium to long-term technology strategies for technological problems and promotion of technology development and commercialisation towards solution of

future social challenges (including the ageing society and vitalisation of local communities), the review meeting to study ICT technology strategies has already been held since December 2017.

Riding the wave of IoT research, Japanese companies are doing very well in terms of Industrial IoT products, services and manufacturing practices across their industries as well as exporting their IIoT products and services to the rest of the globe. In the Japanese industry, utilisation of IoT is spreading along with IIoT for individuals as well as businesses. IIoT for industry brings many contributions such as improvement of company productivity, improvement in the quality of manufactured goods and reduction in labour costs. Specific fields of application include agriculture, construction, tourism, transportation, healthcare and many others.

Internet of Things has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of Radio Frequency Identification (RFID), wireless, mobile and sensor devices. A wide range of industrial IoT applications have been developed and deployed in recent years as reported in [19]. As an activity group to promote IIoT for industries in Japan, the Smart IIoT Promotion Forum was established in 2015, and more than 2400 organisations such as Sony Corporation, Toyota Motor Corporation and Japan Microsoft Corporation joined them. In Europe, Japan and Korea, governments are playing an important role in IIoT planning and deployment [20].

In this section, we discuss some of the Japanese companies who have successfully embraced the IIoT vision.

### ***2.6.1 Smart Agricultural Crop Management—UPR Corporation***

Crops produced in a vinyl greenhouse during winter are sensitive to cold temperatures and may undergo quality denaturation if the temperature fluctuates. To avoid such catastrophic losses, Japanese company, UPR Corp., developed an Internet of Things system [21] that facilitates temperature control and management. With this system, when unacceptable variation is detected in the temperature in an agricultural house (such as disconnection of the power supply to a remote system, thermostat actuation or shutdown of agricultural boiler), a mail message is transmitted to a supervisor's smartphone. Introduction of this system has reduced agricultural crop management costs and promoted realisation of an efficient temperature management.

### ***2.6.2 Smart Agricultural Water Management—Vegetalia Inc.***

Agriculture is considered to be 'climate-smart' when it contributes to increasing food security, adaptation and mitigation in a sustainable way [22]. Hence, Vege-

talia Inc. is now providing water management support for paddy rice via a system called ‘PaddyWatch’ [23]. It is a monitoring system capable of determining CO<sub>2</sub>, soil temperature and other parameters at the farm fields. This system can confirm crop conditions and notify a supervisor by a smartphone or a tablet without mandating a visit to the farm field. Growing conditions of crops can also be confirmed at a remote location through analysis of parameter data (such as environmental data, cultivation and meteorological data) obtained using sensors of various kinds, and boosted by processing using artificial intelligence. By remote control, workers preferentially patrol an area where crops have not grown as expected—this ensures efficient operation and a reduction of production costs.

Checking of water levels in the paddy fields in real time contributes to great reduction in the patrolling hours. In addition, proper water management prevents a reduction in quality due to high-temperature heat generation, thereby exerting considerable influence on yield and crop quality. With systems such as this, smart agriculture is slowly gaining attention across the globe.

### ***2.6.3 Industrial Production—Tsuchiya-Gousei Limited***

The main business of Japanese company, Tsuchiya-Gousei Co. Ltd., is plastic moulding of parts for automobiles and clocks as well as stationery items such as ballpoint pens. A large variety of goods need to be produced efficiently. Therefore, production lines are often operated 24 h a day, every day. However, the availability of workers during the night-time and on holidays can become a serious issue for the management; the consequent trouble-shooting imposes a heavy burden on the management. Tsuchiya then introduced a relevant Internet of Things system [24]. With this system, the operational activities/schedules of all moulding machines (e.g. time for moulding, operating time, etc.) can be determined. Cameras connected to the network are distributed in the factory and office. The status of a moulding machine that becomes issue of concern can be examined via a smartphone or similar smart device. Using the system mentioned above, confirmation of emergency situations and operating systems can be confirmed promptly, even during night-time. The resultant increase in efficiency is impressive [24].

### ***2.6.4 Industrial Production Management—Hitachi Limited***

IIoT also focuses on safety-critical industrial applications [25]. In terms of production management, a digital twin type solution ‘IoT Compass’ [26] is provided at a production site, supplied by Hitachi. This solution was applied in advance at an automobile manufacturing factory in 2017.

The IoT Compass facilitates the resolution of difficulties, involving more than one process, providing cause analysis at locations where possible defects may occur, and

improving the order production, taking into account the constrained conditions. This system is constructed based on the idea of a digital twin. This concept reproduces events in the physical world relating to the factory in a real-time manner, using digital equipment. Using this concept, a simulation space is constructed representing a factory where actual production is conducted and from where products are shipped. Data scattered in the factory are also linked. Such data are displayed with a treasure map function. This function allows digital data to be used with ease; additionally, it enables all production jobs to be optimised for enhanced effectiveness.

### ***2.6.5 Industrial Printing—New Mind Co. Ltd.***

Edible ink printers are manufactured and sold by New Mind Co. Ltd. Such devices can print fully coloured information on foods such as cookies and rice crackers, and thus, used on food production lines. To date, no means were available to ascertain how their foods are used after they were sold to customers. Given that edible printers are related to food manufacturing, considerations related to hygiene aspects are also required. Therefore, the remaining amount of ink and status of use need to be often checked. Accordingly, proper support should be provided to customers. To resolve any related issues, New Mind Co. developed a framework to handle edible ink printers using Internet of Things in collaboration with another company known as Infocorpus Inc. [27]. Now, the remaining amount of ink and its status can be monitored from a remote location. It is also feasible to provide appropriate verification of the cause of issue of a product at the customer's premises. Customer support is now fulfilled by the timely provision of advice and supplies such as ink based on use status of customers' edible ink printers.

### ***2.6.6 Construction Electricity Saving—Zenitaka Corporation***

The Zenitaka Corporation (in Japan) was founded in April 1931. The company provides general contracting services in Japan as well as internationally. As a part of power saving, e.g. at a work site in a tunnel, electrical equipment such as large machines, tunnel illumination, ventilation fans for dust removal and for prevention of reduction in oxygen concentration and of temperature rise are operated day and night. In this case, consumption of massive amounts of electrical power becomes an important issue. Another concern is ascertaining the precise position of every worker in the tunnel to enhance hazard prevention. To resolve these issues, an IoT-based system called 'Tunnel Eye' [28] was developed. Using this, the site status can be known and monitored using various instruments and RFID tags. In this way, the electrical equipment can be controlled automatically based on the information received.

This system was introduced on a trial basis in 2016 in the Shido Tunnel of the Takamatsu Expressway. Results demonstrate that power consumption was reduced by 20% compared to the conventional level, while still securing worker safety in the tunnel. Results confirmed the practical utility of resolving problems occurring at construction sites in mountain tunnels.

Regarding the safety aspects, even if an emergency state such as occurrence of fire or rock fall happens, the whereabouts of the workers can be easily traced from their work activity history.

### ***2.6.7 Garbage Collection Related Solutions—KDDI Corporation***

The KDDI Corporation is a Japanese telecommunications operator formed through the merger of DDI Corp. (Daini-Denden Inc.), KDD (Kokusai Denshin Denwa) Corp. and IDO Corp in October 2000.

KDDI Corp. (Designing the Future) developed an IoT system [29] for the resolution of garbage collection related issues on Kokusai street in Naha City and Okinawa. The garbage bins have an embedded mechanism such that garbage could be collected before overflowing. A distance sensor, a temperature sensor, RaspberryPi and an LTE-M communication module are provided to the IoT-based garbage bin. The amount of garbage accumulated is measured by the distance sensors, with correction done by using a temperature sensor and RaspberryPi. The obtained data are sent to the server to monitor when the garbage bin might overflow. When the garbage in the bin exceeds 80% of the available space, the person in charge of collection will receive a notification. At the garbage bin monitoring centre, the bin status can be checked by colour and by numerical figures from the data received.

A verification test of this system was performed in September 2017. The constructed ‘Overflow prevention garbage bin’ was placed on Kokusai street. Use of the technology was tested and verified on site under actual environmental conditions to assess the quality of communications between relevant sensors to ascertain its feasibility, validity and practical realisation. Results demonstrated that garbage bin information and position information of the collection team were known in the real. The resultant sightseeing solutions to garbage collection system, designed by KDDI Corp., were highly encouraging.

### ***2.6.8 Inspection of Products—Yamato System Development Corporation***

The logistics outsourcing division of Yamato System Development (in Japan) spent many labour hours and much time on the inspection of catalogs, brochures, manu-

als and package inserts of pharmaceutical products, without product identification information such as barcodes. It has been pursuing efficiency improvements for sometime. Previously, several experienced operators equipped with ‘eye for inspection’ checked products manually during final inspection before shipment, performing read-throughs twice, sometimes thrice. Eventually, a shipping instruction and a slip were attached with a string for shipment.

Yamato System has now introduced an IoT system [30] to improve the efficiency of these previously manually executed procedures. With the IoT-based new system, each item is identified by verifying an image of a product captured by a camera mounted on the working bench with image information of the item registered in advance. At the same time, object weight is measured by a weight scale mounted on the working bench, which verifies the weight information of goods registered in advance. Using the system, the company estimates that it is possible to reduce the number of workers by 20%; and monetary costs and time also by around 20% [30].

### ***2.6.9 Logistics Management of Machinery—Toyota Motors Limited***

Toyota Motors Ltd. had about 2700 machine tools and 2000 industrial machines. So, they introduced a ‘Factory IoT’ system [31] aimed at strengthening the businesses logistics solution through a unification of an IoT forklift database, having the integrated management of forklifts working at several hubs in the world and realisation of services involving predictive maintenance. Using this system, the time band of forklift operations, battery efficiency and other important information are determined and displayed. Using this information, customers can work out improvement plans to be carried out at various sites—plans such as effective utilisation of forklifts, reallocation of machinery and personnel at the sites. Result was an impressive improvement in logistics management activity.

### ***2.6.10 Medical Care—Tokyo Women’s Medical University***

At the Tokyo Women’s Medical University, a smart dispensary [32] collects medical information and presents and displays it as ‘Time-series medical treatment record’ to allow medical doctors, and engineers outside the operating room, to share information, thereby helping to contribute to the improvement in efficiency of treatment and safety. Information collected by this system can be analysed employing big data analytics. It is beneficial for maintenance and management aspects such as prevention of operational mistakes, early detection of equipment malfunction and cost management. Besides, remote operations based on data collected by other medical doctors can also be made possible by it.

## 2.7 Literature Analysis

Over the recent years, many informed discussions have taken place during business meetings, conferences, doctoral colloquiums and symposiums on Industry 4.0. An enormous volume of information is available in the form of research articles, book chapters, books, corporate whitepapers, audios, videos and blogs on the use of the IoT paradigm. However, the published academic literature is predominantly valued for its empirical evidence, rather than numerical, for this highly attractive phenomenon.

The use of Scopus and Google Scholar, in addition to Web of Science, helps to reveal a more accurate and comprehensive picture of the scholarly impact of contributions [33]. As per author's own investigation, by the end of 2018, there were 3045 results on smart factories, IIoT or Industry 4.0 from the Web of Science database. Out of these, journal papers are 1167, conference proceedings 1786, review papers 83, editorial material 46 and one book review. Moreover, every country is encouraging new academic manufacturing process literature, as is clear from country-wise analysis. Largest number of papers from various countries (Fig. 2.1) is as follows:

- People of Republic of China (307)
- United States of America (192)
- Germany (124)
- South Korea (102)
- Italy (81)
- England (77)
- Spain (68)
- Sweden (48)
- India (48)
- Taiwan (47)
- France (40)

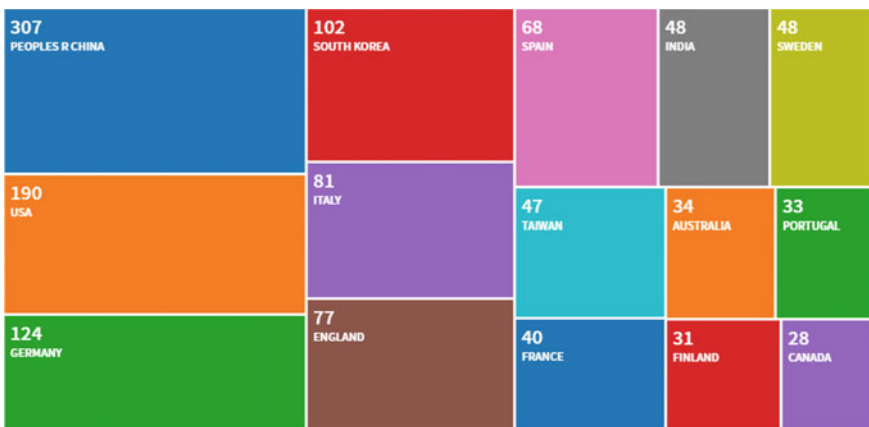


Fig. 2.1 IIoT countrywise publications—analysis chart

- Australia (34)
- Portugal (33)
- Finland (31)
- Canada (28).

This analysis has been represented in Figs. 2.1 and 2.2. Figure 2.1 depicts the contributions of authors on the IIoT phenomenon based on the aforementioned database. It clearly shows that the authors from China were engaged to research and rigorously publish. The chart given given as Fig. 2.2 showcases the 15 most active authors in this domain. This has been generated from the ‘Web of Science’ database analysis report.

Apart from the Web of Science academic and research database on IIoT, we have also drawn patent analysis using the ‘Relecura’ tool [34, 35]. From the analysis, we found that, since the inception of IIoT, there has been a tremendous growth in terms of patents. This is illustrated in Figs. 2.3 and 2.4.

Figure 2.3 represents the patent analysis with respect to various subject areas, e.g. security, power supply, automatic transmission, etc. Among the patents, the blue colour (in Fig. 2.4) refers to the total filed patents since 1988 while green colour indicates the total number of published patents over a while. The yellow coloured line represents the number of patents grants by the authorities. Sky blue coloured line represents expired patents. The graph analysis shows that from 2014 onwards, the Smart Factory concept captured the market due to its research & development and promotional activities.

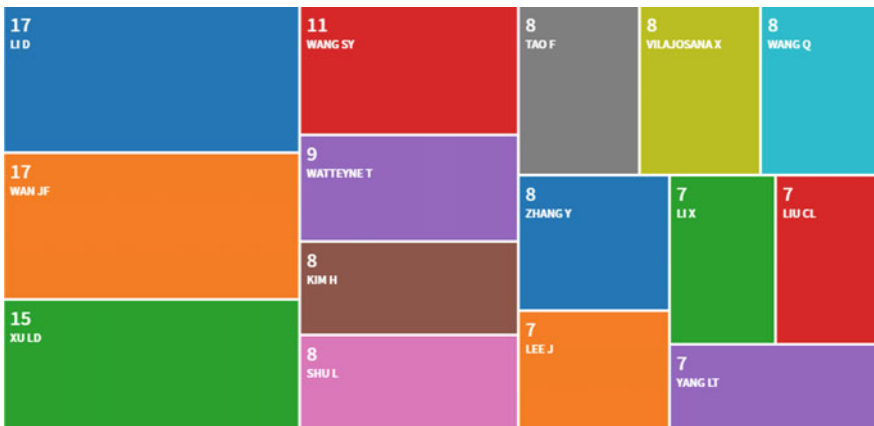


Fig. 2.2 IIoT—authors-wise publications—Top 15



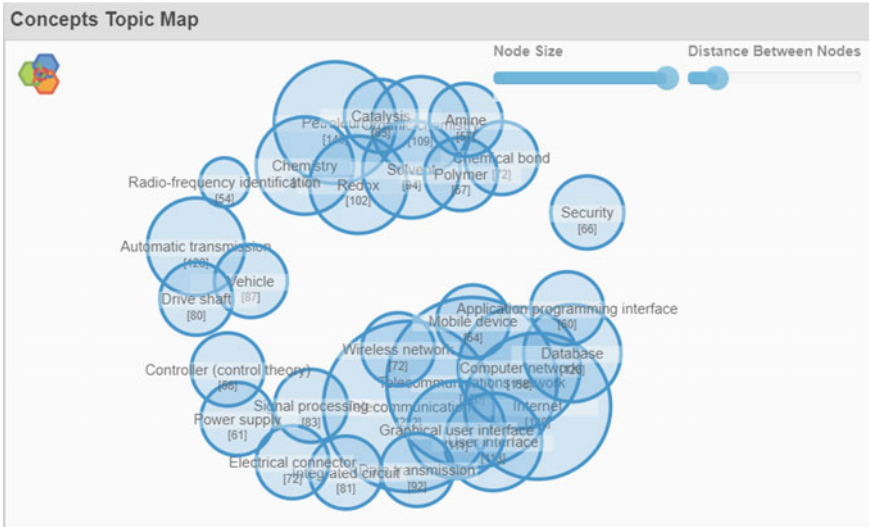


Fig. 2.3 Relecura patent analysis—subject-wise data analysis

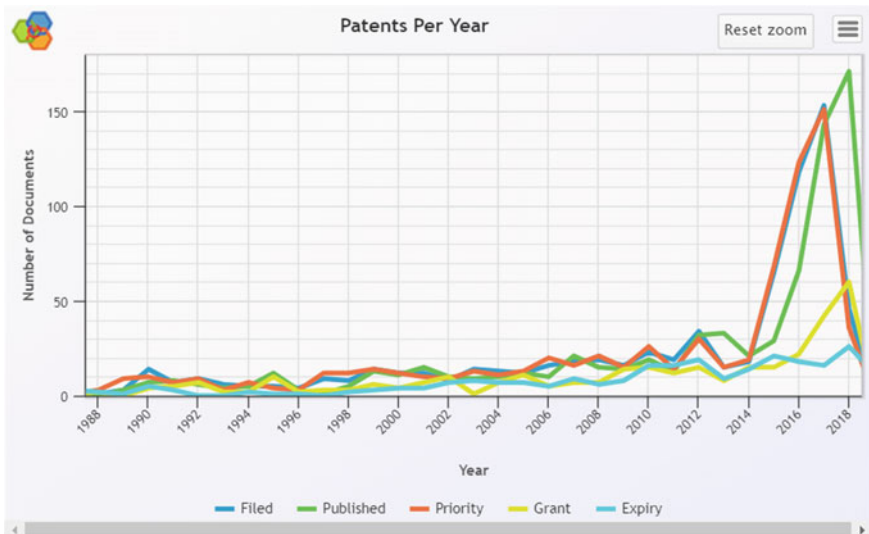


Fig. 2.4 Relecura patent analysis: year-wise data analysis

## 2.8 Methodology

This chapter aims to address the global audience including academicians, researchers, business people, industrial engineering students, mechanical engineering graduates, and manufacturing management professionals, who are looking for in-depth knowledge of the IIoT paradigm and its usage. The fundamentals were observed from different research manuscripts, blogs, corporate white papers, and subject videos. The major databases considered were Scopus, Google Scholar and Thomson Reuters [36]. The main keywords used to search were Industrial Internet of Things, Industry 4.0, smart factory, Industrial Internet, IIoT, and Digital factory.

The book chapter was authored in collaboration with an esteemed Indian-Japan academicians. This collaboration has led to the article exploring the fundamentals of Industrial IoT and illustrating a few novel test cases from Japan.

Almost 7–8 months were taken to compose this book chapter with detailed technical discussions on subject interoperability helping to shape it. The collected data is secondary and qualitative, and the manuscript has been composed and narrated thematically. Hence, the main themes discussed here are Industrial Internet of Things evolution, definitions, applications and test cases from across the globe, though mainly from the industry in Japan.

## 2.9 Conclusion

Technologies play an important role in our day-to-day activities as well as for business and industry. Similarly, the new dawn of Industry 4.0 or Industrial Internet of Things (IIoT) is aiming to embed technology into all the various industrial processes and machinery for automation and operational efficiency.

The IIoT paradigm is widely considered to be one of the primary trends affecting industrial businesses today and in the future. Industries are pushing to modernise systems and equipment to meet new regulations, to keep up with increasing market speed and volatility, and to deal with disruptive technologies like the IoT. Businesses that have embraced the IIoT have seen significant improvements towards safety, efficiency, and profitability.

It is expected that this trend will continue as IoT technologies are more widely adopted. Indeed, the IoT Technologies are serving as bases for this paradigm shift, for example, robotics, sensors, actuators, controllers, RFID, and other electronic computational devices to tag the material, methods, and people in the factories. Various algorithms are at work behind this phenomenon which were developed in C, C++, C#, Java, R, Python etc., using AI and machine leaning processes.

The IIoT brings new growth opportunities to many companies. However, there are technical challenges and important hurdles to overcome, as well, particularly in relation to device connectivity, security of networks, and international standards. Still, global standard institutes like IEEE, ITU, ISO and ANSI are working towards

technological standards and especially device interoperability, including security of data at the time of production of such data. The emerging Industrial Internet will, no doubt, add new energy to the world of industrial products and services in the forthcoming years. However, to be a viable stakeholder as well as a partner in the digitally contestable future and to generate new avenues, companies will need to further evolve to become more technologically based.

## References

1. Davis J, Edgar T, Porter J, Bernaden J, Sarli M (2012) Smart manufacturing, manufacturing intelligence and demand-dynamic performance. *Comput Chem Eng* 47:145–156
2. Thoben KD, Wiesner S, Wuest T (2017) Industrie 4.0 and smart manufacturing—a review of research issues and application examples. *Int. J. Autom. Technol* 11(1)
3. Wan J, Tang S, Shu Z, Li D, Wang S, Imran, M, Vasilakos AV (2016) Software-defined industrial internet of things in the context of industry 4.0. *IEEE Sens J*, 16(20):7373–7380
4. Jeschke S, Brecher C, Meisen T, Özdemir D, Eschert T (2017) Industrial internet of things and cyber manufacturing systems. In: *Industrial internet of things*. Springer, Cham, pp 3–19
5. Umachandran K, Jurčić I, Della Corte V, Ferdinand-James DS (2019) Industry 4.0: the new industrial revolution. In: *Big data analytics for smart and connected cities*. IGI Global, pp 138–156
6. Dujovne D, Watteyne T, Vilajosana X, Thubert P (2014) 6TiSCH: deterministic IP-enabled industrial internet (of things). *IEEE Commun Mag* 52(12):36–41
7. Fuhr PL, Morales Rodriguez ME, Rooke S, Chen P (2017) Convergence and commercial momentum-industrial internet of things evolution. *InTech* 2017(2)
8. MPC (2018) The race towards industry ready, set, go! <http://www.mpc.gov.my/industry4wrld/>. Accessed on 2/3/2019 <http://www.mpc.gov.my/wp-content/uploads/2018/11/The-Race-Towards-Industry-4.0.pdf>
9. Qin J, Liu Y, Grosvenor R (2017) A categorical framework of manufacturing for Industry 4.0 and beyond. *Procedia CIRP* 52:173–178
10. Potgieter P (2017) IIoT Sensors: making the physical world digital. <http://www.ee.co.za/article/iiot-sensors-making-the-physical-world-digital.html>. Accessed on 23/9/2018
11. Dujovne D, Watteyne T, Vilajosana X, Thubert P (2014) 6TiSCH: deterministic IP-enabled industrial internet (of things). *IEEE Commun Mag* 52(12):36–41
12. Jayaram A (2016, December). Lean six sigma approach for global supply chain management using industry 4.0 and IIoT. In: Schneider S (ed) 2nd international conference on Contemporary computing and informatics (IC3I). IEEE, pp 89–94
13. Geng, H. (2017), The industrial internet of things (IIoT) applications and taxonomy. In: *Internet of things and data analytics handbook*. Wiley Publications, pp 41–81
14. Brusakova IA, Borisov AD, Gusko GR, Nekrasov DY, Malenkova KE (2017, February) Prospects for the development of IIOT technology in Russia. In: *Young researchers in electrical and electronic engineering (EIConRus)*, 2017 IEEE conference of Russian. IEEE, pp 1315–1317
15. Al-Ali AR, Zualkernan IA, Rashid M, Gupta R, Alikarar M (2017) A smart home energy management system using IoT and big data analytics approach. *IEEE Trans Consum Electron* 63(4):426–434
16. Hossain MS, Muhammad G (2016) Cloud-assisted industrial internet of things (IIoT)-enabled framework for health monitoring. *Comput Netw* 101:192–202
17. Al-Turjman F, Alturjman S (2018) Context-sensitive access in industrial internet of things (IIoT) healthcare applications. *IEEE Trans Industr Inf* 14(6):2736–2744

18. Japan ministry of internal affairs and communication, Information and Communications in Japan, White paper 2018, Accessed on 23/5/2018 from the Universal Resource locator <http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2018/2018-index.html>
19. Da Xu L, He W, Li S (2014) Internet of things in industries: a survey. *IEEE Trans Industr Inf* 10(4):2233–2243
20. Parwekar P (2011, September) From internet of things towards cloud of things. In: 2nd international conference on computer and communication technology (ICCCCT). IEEE, pp 329–333
21. UPR Corporation, Introduction of IoT to temperature control of vinyl greenhouse, <https://www.upr-net.co.jp/iot/casestudy/usecase-5.html>. Accessed 28 Sep 2018
22. Neufeldt H, Jahn M, Campbell BM, Beddington JR, DeClerck F, De Pinto A, ... LeZaks D (2013) Beyond climate-smart agriculture: toward safe operating spaces for global food systems. *Agric Food Sec* 2(1):12
23. Vegetalia, Inc (2018) Paddywatch, <https://field-server.jp/paddywatch/>. Accessed 2, Sep 2018
24. Systemcreate Co. Ltd. Actual status of data collection of production process and advantages of introduction of IoT. [http://www.systemcreate-inc.co.jp/products/it/iot\\_dnc/iot\\_visualize.html](http://www.systemcreate-inc.co.jp/products/it/iot_dnc/iot_visualize.html). Accessed on 3 Nov 2018
25. Wang H, Osen OL, Li G, Li W, Dai HN, Zeng W (2015, November). Big data and industrial internet of things for the maritime industry in northwestern norway. In: TENCON 2015–2015 IEEE region 10 conference. IEEE, pp 1–5
26. Hitachi Ltd IoT Compass <http://www.hitachi.co.jp/New/cnews/month/2018/10/1017.html>
27. New Mind Co. Ltd (2018) <https://www.sensorcorpus.com/casestudy/newmind>. Accessed 23 Dec 2018
28. Nikkei Business Publications (2018) IoT system introduced to construction site, safety management and electricity saving realized by advanced idea, <https://special.nikkeibp.co.jp/atcl/TEC/16/062300029/>. Accessed on 23 Dec 2018
29. KDDI Corporation (2018) People in the sightseeing area are smiling, people in charge of setting and people walking streets are also smiling. Amount of garbage is notified to prevent overflowing of the garbage bin, [https://iot.kddi.com/cases/okinawa\\_trash/](https://iot.kddi.com/cases/okinawa_trash/)
30. NEC (2018) Example of introduction of image weight and finished product inspection support system, [https://jpn.nec.com/case/nekonet/images/catalog\\_nekonet.pdf](https://jpn.nec.com/case/nekonet/images/catalog_nekonet.pdf). Accessed 30 Dec 2018
31. JDIR (2018) Target of Toyota Industries Corporation promoting IoT of forklifts in the world, <http://jbpres.ismedia.jp/articles/-/52881>. Accessed 31 Dec 2018
32. AMED (2018) Japan agency for medical research and development. Smart Cyber Operating Theater (SCOT). Accessed 11/11/2018, [https://www.amed.go.jp/news/release\\_20180709-01.html](https://www.amed.go.jp/news/release_20180709-01.html)
33. Meho LI, Yang K (2007) Impact of data sources on citation counts and rankings of LIS faculty: web of science versus Scopus and Google Scholar. *J Am Soc Inform Sci Technol* 58(13):2105–2125
34. Biswas R, Banerjee A, Halder U, Bandopadhyay R (2018) Transgenic research in vegetable crops with special reference to Brinjal. In: *Genetic Engineering of Horticultural Crops*, pp 155–167
35. Sarkar S, Banerjee A, Halder U, Biswas R, Bandopadhyay R (2017) Degradation of synthetic azo dyes of textile industry: a sustainable approach using microbial enzymes. *Water Conserv Sci Eng* 2(4):121–131
36. Harzing AW, Alakangas S (2016) Google Scholar, Scopus and the Web of Science: a longitudinal and cross-disciplinary comparison. *Scientometrics* 106(2):787–804

# Chapter 3

## Systems Development for the Industrial IoT: Challenges from Industry R&D Projects



Nuno Santos, Francisco Morais, Helena Rodrigues and Ricardo J. Machado

**Abstract** Industrial paradigms such as Industry 4.0 (I4.0), also known as *Industrial Internet of Things (IIoT)*, provide an insight into the use of underlying Internet of Things (IoT) technologies in an integrated manner. In order to follow the IoT vision and gain the inherent benefits, industrial information systems providers have been modernizing their solutions. However, the complexity of such systems has been proving an obstacle in developing efficient solutions. Following the trends of the industrial IoT including *Smart Manufacturing*, *Connected Factories*, and *Factories of the Future*, industrial and academic projects have also been aiming at developing better solutions for IIoT-related projects. Such solutions typically heavily rely on interoperability requirements between sensors, actuators and other IoT-based diverse smart devices toward, for example, supply chain and production management services such as ERP, MES, and SCADA. This chapter identifies challenges in developing IIoT solutions, based on recent R&D projects. Such identification, in turn, contributes to proposing opportunities, challenges, methodologies, and approaches for the analysis, design, implementation, and deployment of R&D projects. This is specifically so when developing interoperable solutions for the IIoT domain, mainly concerning the applications of the IoT and services to the manufacturing industry.

**Keywords** IIoT · I4.0 · Information systems · Information systems development · R&D challenges · Connected factories · Smart manufacturing · ERP · SCADA

### 3.1 Introduction

Digitization is becoming a business reality for many organizations in sectors such as manufacturing, logistics, oil and gas, energy, transportation, mining, aviation, and many more. As the industry is becoming increasingly more pervasive, the Internet of Things (IoT) in the industrial sector, known as the industrial IoT (IIoT), is now

---

N. Santos (✉) · F. Morais · H. Rodrigues · R. J. Machado  
CCG/ZGDV Institute, Guimarães, Portugal  
e-mail: [Nuno.Santos@ccg.pt](mailto:Nuno.Santos@ccg.pt)

ALGORITMI Center, School of Engineering, University of Minho, Guimarães, Portugal

a reality in the context of industrial transformation. The driving philosophy behind IIoT is that smart machines are better than humans at accurately capturing, analyzing, and communicating real-time data. The underlying technologies include sensing and actuation technology, machine to machine (M2M) communication, distributed computing, machine learning, and artificial intelligence.

A typical IIoT system consists of intelligent systems (applications, controllers, sensors, and security mechanisms), data communication and computing infrastructures (cloud computing, edge/fog computing, etc.), data analytics (to support business intelligence and corporate decision-making), and most importantly, the human element. The benefits that IIoT promises include enhanced safety, better reliability, smart metering, inventory management, equipment tracking, facilities management, and smart environments, etc.

In this scenario, industrial information systems may be seen as complex systems that emerge from technological and business opportunities. They are a fusion between the operational and information computing domains in industry capable to realize the so-called fourth industrial revolution, the Industry 4.0 initiative [1].

This digitalization of business processes within the industrial sector has led to an increase in complexity in technological solutions. IIoT system designers and providers also face new challenges of different natures along the entire product development life cycle, from requirements elicitation and system quality to development and deployment. Requirements elicitation, communication, and maintenance must face complex systems with thousands or even more requirements that involve many new factors and the dynamic participation of multiple stakeholders. This leads to the need for new software architectures that must accommodate heterogeneity of systems, capabilities, domains, and competencies. A common approach to initiate these developments is by using domain reference architectures and standards.

Recent years have seen a rapid increase in the number of reference architectures designed to guide IIoT applications development [2]. Reference models like industrial internet reference architecture (IIRA) [3], industry 4.0 reference architecture model (RAMI 4.0) [4] and NIST smart manufacturing (NIST SM) [5] provide standardized organization of concepts within the modernized industrial environment. Additionally, NIST cloud computing reference architecture (NIST CCRA) [6] is a widely adopted reference architecture toward the deployment of cloud solutions.

To summarize, IIRA, RAMI 4.0, and NIST SM are popular reference models for developing industrial architectures. IIRA and NIST encompass several industrial domains while RAMI 4.0 is focused on manufacturing [7]. Since RAMI 4.0 and IIRA provide their functionality as services by implementing a service-oriented architecture (SOA), industrial digital thread (IDT), and asset efficiency (AE) testbeds are semantically interoperable from a functional point of view between these two architectures [8, 9]. These testbeds relate to real implementations of these reference architectures.

Adopting these reference architectures, however, is not sufficient for providing technical and architectural requirements necessary for developing IIoT systems [10, 11]. Additionally, design and development of such systems should be complemented by architectural design approaches. Model-driven development is already popular

for the development of cloud computing solutions [12], and more recently within the design of fog computing related architectures [13]. Additionally, successful implementation, as reported in literature, relates to specific use cases where industrial internet technologies are being applied, i.e., testbeds based on IIRA and RAMI 4.0. Even though the IDT and AE testbeds allow architecture implementations, using these reference models does not provide technical specifications in an abstraction level for conducting organizational projects, as there is still a lack of proper alignment of technology with the business requirements.

In this chapter, we aim to discuss assumptions, challenges, and approaches with respect to analysis, design, implementation and deployment of IIoT systems for three R&D projects from academia. To support this analysis, we chose a reference model characterized by three design dimensions: requirements elicitation, architecture design, and interoperability. With this approach, we aim to provide a more structured and representative view of the most fundamental design decisions in the chosen projects.

The aforementioned design dimensions have direct implications for the design of IIoT systems and correspond to fundamental issues that any IIoT system needs to address [1, 14]. Very briefly:

- The requirements elicitation dimension is derived from the need for applications developers to contextualize and delimit user actions in a given domain, e.g., engineering. It is a project stage that allows an in-depth knowledge acquisition of the context, say industrial, where the project will be carried out. Such knowledge is advisable due to the complex ecosystem of IIoT projects, e.g., large variety of sensors and devices, machinery (and related controlling systems), communication protocols, data formats, data value, etc. Thus, addressing such complexity without a proper context and domain knowledge will likely lead to a project failure [14].
- The second dimension, that of architecture design, is derived from the need for software architects to model high-level design that satisfy stakeholder requirements and give guidance for application design and development [1].
- The third dimension refers to technical and semantic interoperability. Technical interoperability is derived from the need for software engineers to deal with the integration of different domains with differing communication requirements and with technological heterogeneity of IIoT applications [15]. Semantic interoperability is derived from the need for software engineers to deal with the heterogeneity of IIoT ecosystem's entities and intersection of different IIoT domains [5].

For each of the three dimensions, we review three Portuguese funded research and development (R&D) projects for the IIoT domain. The projects being:

- Integrated management platform 4.0 (IMP\_4.0).
- Unified hub for smart plants (UH4SP).
- Solutions for the industry of the future (PRODUTECH-SIF).

IMP\_4.0 is intended mainly for the textile domain (namely milling, weaving, and clothing processes), UH4SP for the cereal and cement operations (e.g., logistics), and PRODUTECH-SIF for the rock industry (cutting and polishing processes). All

these projects aim at developing interoperable solutions for the industrial market. The focus is on how each system addresses a particular dimension as mentioned above.

The remainder of this paper is organized as follows. In Sect. 3.2, the three Portuguese R&D projects are presented and discussed regarding their industrial settings. In Sects. 3.3, 3.4 and 3.5, we analyze the chosen design dimensions (requirements, architecture, and interoperability) as described above, ranging from introducing the concept and typical challenges to describing their addressing in the presented projects. Finally, in Sect. 3.6, we summarize our conclusions.

## 3.2 Overview of the Three IIoT Related R&D Projects

In this section, the three R&D projects (viz: IMP\_4.0, UH4SP, and PRODUCTECH-SIF) are briefly described, where the focus is not on the thorough presentation of the project's artefacts or developed tools, but rather on the presentation of the systems development in the context of IIoT with a view to discussing the related challenges. The projects are described in their industrial settings, using widely adopted industrial standard models such as the following:

- ANSI/ISA-95.00-2000 enterprise-control system integration or ISA-95, in short [16].
- Industrial reference models like IIRA [3], RAMI 4.0 [4], and NIST SM [5].

There are mappings and overlaps between the layers and viewpoints of the referred models. Such discussion is presented in the research reported in [9] and [17]. The mapping from these works is summarized in Fig. 3.1, so they are not thoroughly described in this section. Rather, they are used in order to allow a clear understanding of the industrial setting where IMP\_4.0, UH4SP, and PRODUCTECH-SIF projects were conducted.

We believe that using the architectural layers as defined in the standards allows to understand the involved systems that compose the smart manufacturing ecosystem in these projects. Since the standard layers can be mapped with each other, the systems are presented in layers that are familiar to a wide-range of domains (for instance, while RAMI 4.0 is more oriented to European manufacturing industry reality, IIRA is more oriented to a wider range of industries generally from North American region, and finally, ISA-95 focuses more on system interoperability). Thus, in this section, each project is presented by classifying the developed industrial systems within these layers. Finally, when different layers communicate, the required interoperability needs between them are derived. For this reason, the projects description includes the adopted interoperability strategy. We start by briefly presenting each layer or view point of this model viz: ISA-95, IIRA, and RAMI 4.0:

- ISA-95: This model is hierarchical and composed of five business process levels, labeled 4 to 0. viz:



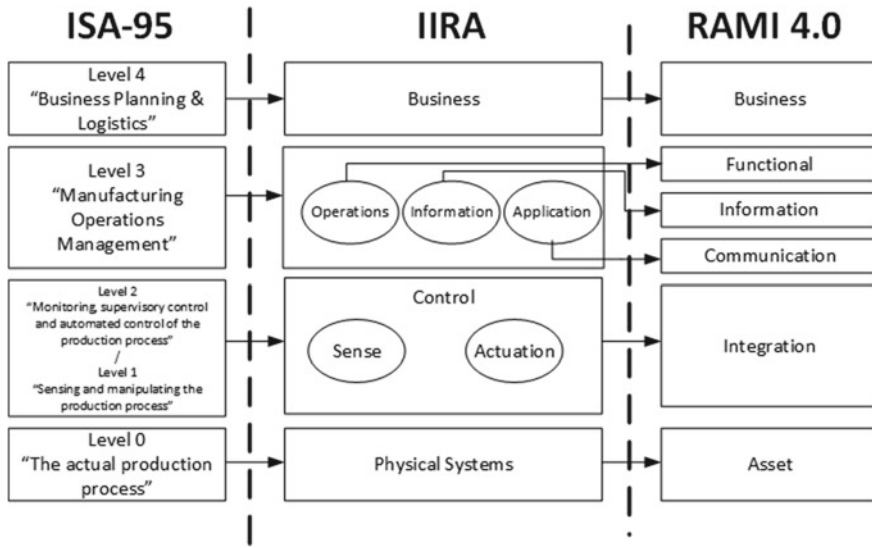


Fig. 3.1 Layer mapping between ISA-95, IIRA and RAMI 4.0 (adapted from [9] and [17])

- Level 4 “Business Planning & Logistics”: typically associated with enterprise resource planning (ERP), customer relationship management (CRM), product lifecycle management (PLM) systems, among others.
  - Level 3 “Manufacturing Operations Management”: typically associated with manufacturing execution systems (MES), material resource planning (MRP), among others.
  - Level 2 “Monitoring, supervisory control and automated control of the production process”: typically associated with supervisory control and data acquisition (SCADA) and human-machine interface (HMI) systems.
  - Level 1 “Sensing and manipulating the production process”: associated with programmable logic controller (PLC) systems.
  - Level 0 “The actual production process”: referring to the machines, devices, and the resources that physically transform raw materials to the desired product.
- IIRA: This is composed of business, usage, functional, and implementation viewpoints. However, the projects classification only fits within the functional viewpoint, which relates to “Business,” “Operations,” “Information,” “Application,” “Control,” (sense or actuation) and “Physical Systems.”
  - RAMI 4.0: This model presents a three-axis classification, composed of vertical systems, facilities and products lifecycle, and hierarchy levels for different functionalities within factories or facilities. Only the vertical axis is used for describing the projects.

NIST SM is composed of product, production, and business viewpoints, which are merged in the form of a “manufacturing pyramid.” This pyramid relates to a hierarchy

of systems, which follows the ISA-95 levels, thus for that reasons it was not included in Fig. 3.1. Whenever the systems are classified under different levels, it implies that there is a need for addressing interoperability between levels. The detailed discussion of IMP\_4.0, UH4SP, and PRODUCTECH-SIF projects now follows in the following subsections.

### ***3.2.1 Integrated Management Platform 4.0 (IMP\_4.0)***

The IMP\_4.0 platform enables a software-house (F3M information systems, SA, located in Braga, Portugal) to optimize the development process of delivering solutions to their customers with tools to support decision-making processes. The solutions are based on public and private clouds, which are interoperable with devices in an IoT and Cyber-Physical Systems (CPS) approach.

The IMP\_4.0 project is about an ERP system for the textile production domain, where the focus is on support milling, weaving, and clothing processes, by providing a set of reusable and integrated software modules. Additionally, the platform's development includes establishment of generic modules and variability management for enabling its extension to textile, footwear, cutlery, metal-mechanic, glassware, and other related sectors. In terms of the development, the IMP\_4.0 project includes development of the following:

- a set of management ERP-based features for the manufacturing sector to be delivered to customers
- cloud-based microservices for process execution
- shop floor software services for manufacturing processes, e.g., control of production lines, and instructions for cutting machines.

For the ERP-based features and supporting microservices architecture, we are referring to the business layer of IIRA and RAMI 4.0, and level 4 of ISA-95. Regarding the shop floor services, which deal with the production data generated within the processes performed at the production lines, we refer to the control layer of IIRA, integration layer of RAMI 4.0, and levels 2 and 1 from ISA-95. The specification and design strategy of these features and services are discussed in Sects. 3.3 and 3.4.

Communication between them is based only at technical interoperability strategy, involving developing the APIs and using REST protocols between ERP features and microservices; and AMQP messaging between production orders and production actuators. A broader discussion is presented later in Sect. 3.5.1.

### ***3.2.2 Unified Hub for Smart Plants (UH4SP)***

This project aims at developing a platform from distributed industrial unit plants, with focus on the cement production domain, allowing the use of data acquired from

IoT systems for enterprise-level production management and collaborative processes between plants, suppliers, forwarders, and clients. The project aims at developing new solutions regarding the control of trucks arrival/departure as well as the load/unload activities, and for communicating with the plant's ERP system and the industrial hardware. These solutions are validated within a proof of concept performed in an ecosystem of industrial unit plants using production management systems developed by Cachapuz Bilanciai Group, located in Braga, Portugal, as they are the leading entity of the UH4SP project consortium.

The UH4SP project arose from the need of overcoming Cachapuz solution's limitations in adopting the IIoT paradigm. Initially, the current solution was deployed on-premises. It has a considerable scaling and complexity, which made it inadequate and inflexible to enable the development and deployment of cloud services based on modules and external access. The on-premise deployment poses a difficulty for promoting a corporate-level management, since in order for the industrial group manager to have an integrated analysis of the group's plants, the manager is only able to access the individual plant's ERP one at a time using a remote virtualized environment. The remote business analysis is also impossible to perform in some contexts, e.g., within the plants that are located in poor Internet connectivity spaces. The current solution did not enable the incorporation of remote technical interventions. Thus, the current solution was not able to respond to a previous need of enabling third-party access (e.g., forwarders, customers, suppliers) to the inclusion of collaborative tools in process execution and analysis. To reiterate, the UH4SP project is aimed at developing the following:

- new functionalities for providing management of corporate-level production
- tools for supporting new collaborative processes within the supply chain
- a microservices architecture
- production management services that rely on previous synchronization of Cachapuz's systems (at the industrial unit level).

The management of corporate-level production, tools for collaborative processes within the supply chain and the microservices architecture refer to business management support. Hence, these are classified under the business layer of IIRA and RAMI 4.0, and at level 4 of ISA-95. The production data at the industrial unit level are acquired from a MES; hence, this is classified under the operations layer of IIRA, functional layer of RAMI 4.0, and at level 3 of ISA-95.

The communication between these systems is addressed in UH4SP via the technical interoperability strategies. Here, communication between the web applications and the microservices is based on RESTfull invocations between the APIs. Here, the project's middleware (an API gateway) is responsible for acquiring the data at the industrial unit level and providing it to the cloud-level microservices. Synchronization between the cloud and the industrial unit level is implemented using MQTT protocols. A broader discussion appears later in Sect. 3.5.1—further detail can also be found in [18].

### 3.2.3 *Solutions for Industry of the Future (PRODUTECH-SIF)*

The umbrella project “programa mobilizador PRODUTECH-SIF—Soluções para a Indústria do Futuro” (Solutions for Industry of the Future) embodies a comprehensive response toward the development and implementation of new production systems, embedding advanced production technologies that contribute to the challenges and opportunities of the fourth industrial revolution (I4.0). It is a program for the Portuguese industrial sector, aimed at the development of new production technologies for multi-sectorial applications. The program is composed of a set of projects, encompassing the following:

- Networked production systems
- Innovative technologies for new cyber-physical production systems
- Development, management, and improvement of cyber-physical production systems (CPPS)
- Key enabling production technologies, automation, and advance robotic systems
- Integral sustainability and efficiency of production systems
- Energy-related technologies
- Advanced tools for the development of products and services.

This chapter focuses on the network production systems (NPS) project. NPS results from the need to create adequate conditions for the networking of production systems, respective industrial equipment, and business information systems, allowing interoperable, coordinated, and/or integrated operations. This activity contributes to the overall scope of the project through a clear and comprehensive identification and characterization of architectures and reference solutions supporting the realization of an integrated network production environment and the exploitation of the information made available through CPPS. This project outputs a NPS semantic interoperability platform (cf. Sect. 3.5.2), contributing to two typical IIoT testbeds [9]: industrial digital twin (IDT) and asset efficiency (AE).

The NPS projects are different from the previous projects, since the goal is to develop a platform for integrating systems rather than providing solutions for supporting the business of a specific organization. The current project defines a scenario regarding rock cutting and polishing, consisting of defining the process needs (within production orders), identifying product needs (from design specifications) and monitoring and control of the production process to fulfill the orders (based on data acquired from actuators in the production line). This project also includes the integration of ERPs, MES, and Actuator devices.

For ERPs, the classification refers to business layer of IIRA and RAMI 4.0, and level 4 of ISA-95. For MES, the classification refers to operations and application layers of IIRA, functional layer of RAMI 4.0, and level 3 of ISA-95. For actuator devices, which mainly control the process, they fit under the control layer of IIRA, Integration layer of RAMI 4.0, and levels 2 and 1 of ISA-95.

This was the only project, among the three included in this chapter, to address both technical (cf. Sect. 3.5.1) and semantic (cf. Section 3.5.2) interoperability.

### 3.3 Requirements Elicitation

Requirements elicitation in IIoT projects, like any other projects from other domains, provides information regarding the business needs that become the basis for further design and implementation of the projects [14]. In complex ecosystems like the ones relating to IIoT, proper analysis of functionalities, processes, data flows, etc. is highly crucial.

In the requirements elicitation phase of system development, a characterization of the “as-is” situation is performed and the needs determined. Typical examples of this exercise are the modeling of an enterprise’s business processes [e.g., using business process modeling notation (BPMN)], identification of technical and/or product glossary, determining relationships between main domain concepts, and specifications of the structure of the involved systems.

Even when the aim is to perform the characterization of the “to-be” situation, it is advisable that the requirements elicitation is conducted first to include a proper domain characterization, by analyzing the business processes, the information (data), and the systems (hardware/software) that compose the ecosystem. The business process analysis (using BPMN or any other business process notation) must reflect the enterprise’s vision toward the IIoT paradigm and where the information to integrate must be depicted.

In this context, process reference models have an interesting useful role in requirements elicitation. For instance, it is common that manufacturing sector follows supply chain operations reference (SCOR) [19] for defining the processes for managing the supply chain (plan, source, make, deliver, return, and enable processes). These reference models are often composed of processes, subprocesses, roles, tasks, operations, that may easily be mapped in a business process notation language [20]. It is not expected that an enterprise follows only one reference model. For instance, the GS1 global standard for traceability is widely adopted for carrying out tasks for product traceability [21], and may be adopted as well.

Any software project is carried out in one of these contexts: a greenfield project (i.e., from scratch), or alternatively, a brownfield project (i.e., with existing legacy systems). If an IIoT project aims at replacing a given system or otherwise collaborating with it, the legacy system should be properly characterized, as well as the current business processes and data flows that the system supports.

#### IMP\_4.0 Project

Within the IMP\_4.0 R&D project, the entire software product management, from identification of market needs to assets identification to release/version management, was considered the initial domain of engineering, where it was intended to

characterize the processes of the spinning, textile and garment domains, in terms of commonalities and domain variabilities. The software requirements for the identified processes resulted in a specification of UML use cases. The use case model was composed of the following use cases related to the ERP's modules: stocks sales, purchases, production, planning, outsourcing, quality control, packing list, finances, and stakeholder management. Additional use cases related to integration with cloud infrastructures, based on NIST CCRA, were also included. Each use case was refined in functional decomposed use cases, resulting in 86 low-level (also called leaf) use cases, i.e., the ones that were not further divided.

### **UH4SP Project**

Within the UH4SP project, the business information that serves as input for requirements was gathered: this being business needs, project goals, vision document, etc. Techniques like interviews, questionnaires, and workshops were additional and complementary approaches to the aforementioned document analysis for gathering inputs on requirements. Reference models also served as inputs to the requirements phase. Cloud computing reference models such as NIST CCRA [6] were also input for cloud-related functionalities [22]. The fog computing issues were based in the architectural layers such as in [23], e.g., business applications, cloud management, fog management, fog infrastructure, and IoT systems.

The requirements elicitation started at listing a set of stakeholder expectations toward the product roadmap, encompassing the entire product. This task output 25 expectations categorized by environment, architecture, functional and integration issues, which relate to business needs that afterward promoted the discussion of scenarios. The stated project objectives referred to the following:

- defining an approach for a unified view at the corporate (group of units) level
- developing tools for third-party entities
- assuring in-plant optimization
- assuring system reliability.

This task output fifteen modeled scenarios, divided into four groups that relate directly to the project's four objectives. Then, a set of UML use cases were modeled based on those scenarios and decomposed resulting in a total of thirty-seven use cases.

### **PRODUTECH-SIF Project**

The NPS platform of PRODUTECH-SIF is a service-oriented architecture (SOA) for manufacture and based on the concepts of IoT and CPS. The platform focuses on the collection of information based on a sensor installed in the equipment and the bidirectional interaction allowing users to control the processing of materials. The requirements elicitation task encompassed the definition of a main scenario that described a rock cutting and polishing process in a "to-be" setting, where ERP, MES and sensors communicate the production information with each other. In order to properly define the scenario, the "as-is" specification was determined in terms of the

functions performed by the equipment, specifications of the information (included in each system concerning the cutting and polishing process), and eliciting the functionalities for resources management by the platform.

### 3.4 Architecture Design

Now that the requirements phase is performed and the solution needs are identified and properly specified, the next step relates to designing the system.

System design is typically performed using a model, e.g., an architecture. However, architecture design should be addressed as an iterative process, as design should start at a conceptual level and refined until it is detailed enough; which is to say that the abstraction level goes from higher level abstraction to low level abstraction during this process [14]. This mechanism is in line with the design process proposed by Douglass [24].

Architectural design defines the strategic decisions that affect software components, such as concurrency model and the distribution of components across processor nodes. Mechanistic design elaborates individual collaborations by adding “glue” objects to bind the mechanism together and optimize functionality. Such objects include containers, iterators, and smart pointers. Detailed design defines the internal structure and behavior of individual classes. This includes internal data structuring and algorithm details.

Besides, IIoT projects may heavily rely on technology. However, the developed system is of little use if it is unable to address the business needs. For this reason, it is necessary that the architectural design is performed initially at a conceptual level. At this point, some design decisions are made, e.g., to define separation of concerns. Here, we have several architectural patterns that can be considered by an IIoT system, for instance three-tier, Gateway-mediated edge connectivity, or layered databus. The implementation viewpoint of the IIRA model is a valid example for adoption at this point. It is the IIRA viewpoint that is oriented towards architecture-related decisions. This viewpoint adopts the three-tier architecture, as systems and services are deployed in an enterprise, platform, and edge tier.

Numerous enabling technologies also have reference architectures that allow making architectural design decisions. The implementation of cloud computing architectures, for instance, may be based on the NIST CCRA [6] model. The building of IoT systems in these settings often leads to developing intermediate systems, for instance, fog computing architectures. In these cases, the OpenFog reference architecture (OpenFog RA) by OpenFog consortium [25] also allows the adoption of a tier structure for separating concerns as cloud, fog, and edge computing. Additionally, other reference models like ETSI MEC (Mobile Edge Computing), OPC UA, open connectivity foundation (OCF), OpenNFV, etc. may also be adopted. It is also worth suggesting that these models are complementary to IIRA and OpenFog.

A typical concern in architectures with such complexity in the IIoT context is the alignment with the business requirements. Some known methods that support archi-

itecture design with such alignment are: Reuse-driven software engineering business (RSEB) [26], family-oriented abstraction specification and translation (FAST) [27], feature-oriented reuse method (FORM) [28], *Komponentenbasierte Anwendungsentwicklung* (or *KobrA*—that is German for “component-based application development”) [29], quality-driven architecture design (QADA) [30], product line software engineering (PuLSE) [31], and four step rule set (4SRS) [32].

As the architecting process aims at detailing the design, the goal is to specify the behavior of specific components (or services) of the system and how they may interact with each other. At this point, design decisions are based in terms of the architectural style to adopt, the design of components behavior, and how components might interact. Architectural styles relate to adopting, for instance, component based, event-based, service-oriented, or microservices-based styles. The components behavior relates to adopting existing architectural patterns, like object-oriented programming, model-view-controller (MVC), entity-boundary-controller (EBC) or Data, Context, and Interaction (DCI) patterns. Additionally, there are complimentary design patterns that are adopted for specific situations.

There is also a plethora of available handbooks of patterns. For instance, the pattern-oriented software architecture (POSA) introduces a set of design patterns related to concurrency and networking (e.g., event handling, synchronization) [33], resource management (e.g., caching, pooling, etc.) [34], and distributed computing (e.g., message router, publisher-subscriber, broker, client proxy, reactor, etc.) [35].

### **IMP\_4.0 Project**

The architecture design within the IMP\_4.0 project was based on the functional decomposition of requirements using UML use cases, where the 4SRS method was used to support deriving a logical architecture composed by UML components that trace back to each functionality. The 86 leaf-use cases were used as input, which allowed devising 140 components. These components relate the behavior of web applications and a set of supporting microservices, namely: stocks, sales, purchases, production orders, bills of materials, planning, outsourcing, quality control, packing list, checking accounts, banking, and stakeholder management. Each microservice’s behavior is specified based on its constituent components. The 4SRS also allowed identifying the required inter-service communication between the microservices and web applications to perform the business processes. An example of the stocks microservice using SoaML participants is depicted in Fig. 3.2.

### **UH4SP Project**

Within the UH4SP project, after having all the requirements elicited, gathered, modeled, and validated, 37 use cases (cf. Sect 3.3) were used as input for the logical architecture design by using the 4SRS method. The architecture was composed of 77 components, grouped into five major packages, namely [13]: P1 configurations; P2 monitoring; P3 business management; P4 UH4SP integration; P5 UH4SP fog data. The logical architecture diagram was then used to specify microservices, using SoaML service participants, capabilities, service architecture and service interfaces



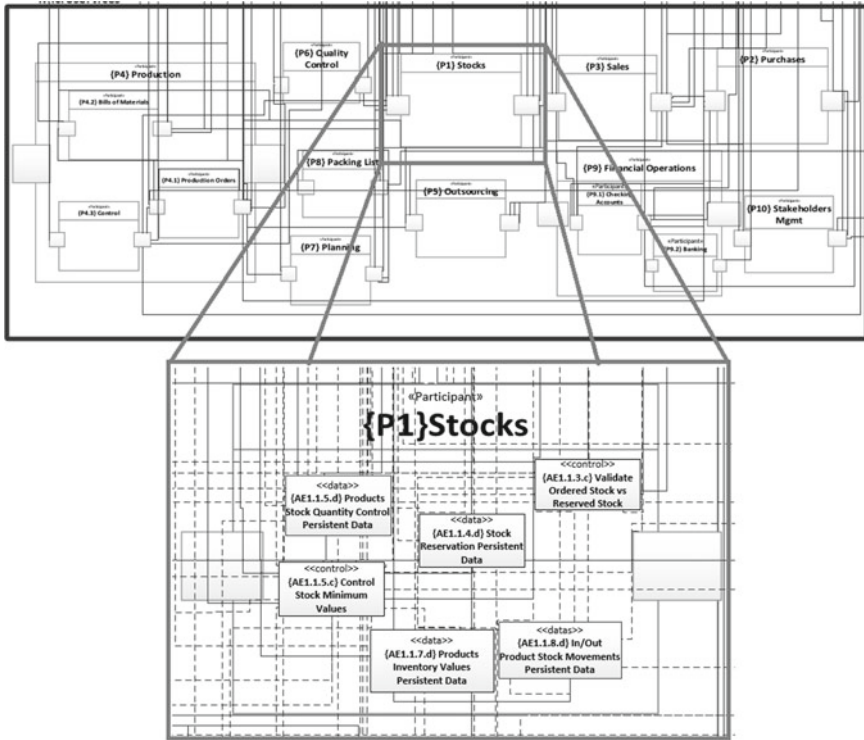


Fig. 3.2 Example of microservice within IMP\_4.0

diagrams [13]. An example of one of the specified microservices responsible for retrieving production data from local industrial units, is presented in Fig. 3.3.

**PRODUCTECH-SIF Project**

Within the PRODUCTECH-SIF (NPS) project, the goal was to define a high-level architecture suitable for the elicited project scenario (cf. Sect. 3.3). For the architecture design, the project considered the three-tier architectural pattern since it does not exclude multiple implementations of the same layer or multiple connections between layers, although each of them is represented once. Using existing literature on architecture compliance with IIRA and RAMI 4.0 [5, 9], the project used the three-tier architecture pattern for guiding the architecture design.

The PRODUTECH-SIF (NPS) project architecture is composed of three layers: edge tier, platform tier, and enterprise tier as explained below—also refer to Fig. 3.4:

- The edge tier includes the manufacturing assets, the edge devices, and edge gateways (CPS developed in the project and sensor devices from manufacturers) which constitute the control domain. The edge tier gathers information from edge nodes such as assets, sensors, or controllers of the system using the network. Edge nodes can communicate with edge gateways thus leading the data to other networks. In

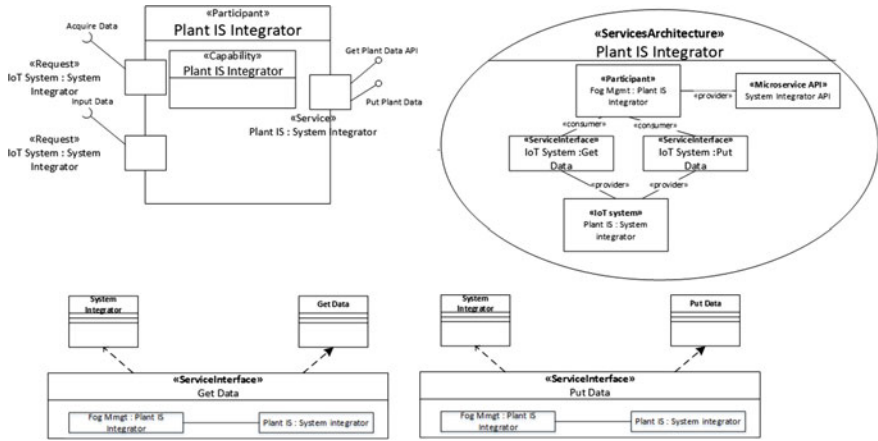


Fig. 3.3 Specification of UH4SP services in SoAML (adapted from [13])

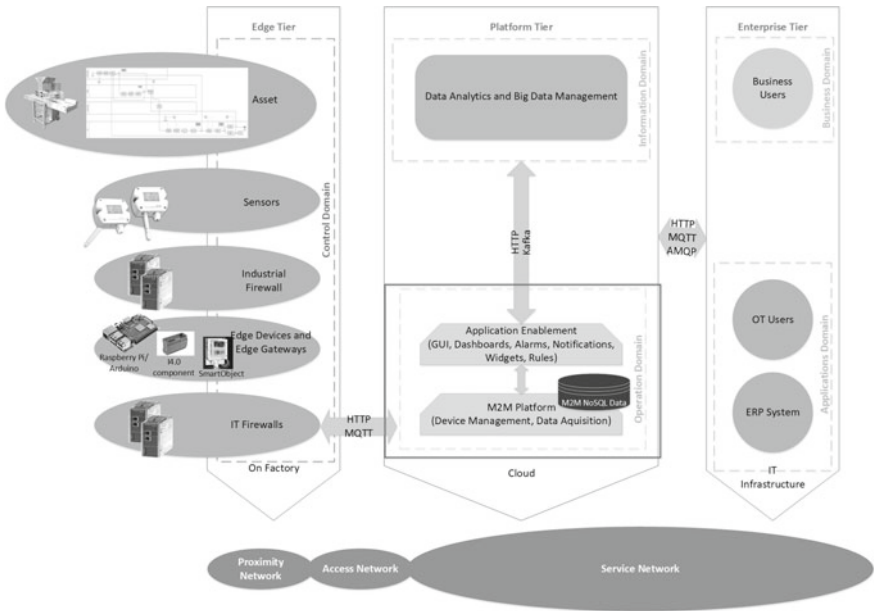


Fig. 3.4 PRODUTECH-SIF (NPS) architecture based on Three-Tier Pattern (adapted from [10])

the industrial digital twin (IDT) testbed, the edge tier encompasses all the assets, firewalls, and devices that integrate the digital thread, providing data related to the asset performance and state that feeds the digital thread. Regarding the asset efficiency (AE) testbed, the asset is integrated with sensors gathering state data regularly and sent to a big data management platform for further predictive analysis of the data.

- The platform tier is the layer between the edge and the enterprise tier. It receives information from the remaining tiers, processes, and forwards information from one tier to the other. The platform tier integrates the assets, the data analysis, and a big data platform to create dashboards, alarms, notifications, etc. In IDT and AE testbeds, the platform could be an IoT system with data transaction supported by machine to machine communications.
- The enterprise tier implements domain-specific applications associated with an asset or factory, as well as decision support systems and interfaces for end users or specific domain users. It receives data from both the edge and the platform tiers and sends control commands to both tiers. The enterprise tier comprises an application domain composed by web portals and user interfaces (e.g., ERP, MES) for communicating with the edge and platform tiers, and a business domain that implements the business.

Just like the three-tier architectural pattern, the three layers of the PRODUTECH-SIF (NPS) project architecture are connected using three types of networks: proximity, access, and service network. The proximity network connects the edge nodes to the gateways through TLS and OPC UA protocols (cf. Sect. 3.5.1). The access network connects the edge and platform tiers using TLS communication protocols. The service network connects the platform services with enterprise services. Additionally, the OPC UA protocol is used between the various devices and the corporate systems.

### 3.5 System Interoperability

In this section, the third design dimension, namely the interoperability, is addressed. Interoperability is one of the fundamental characteristics of IIoT/I4.0 projects; and it is a common fact that many challenges in these projects relate to technical and semantic interoperability. In terms of technical interoperability, Sect. 3.5.1 addresses communication and messaging protocols between cloud applications, cloud services, and industrial applications within the three R&D projects. In terms of semantic interoperability, Sect. 3.5.2 addresses challenges in defining a standardized industrial vocabulary in an ontology and how this ontological model is used within an interoperability platform, where namely, it was only addressed in the PRODUTECH-SIF project.

### 3.5.1 *Technical Interoperability*

According to the new European Interoperability Framework (EIF), included within the Interoperability Solutions for European Public Administrations (ISA<sup>2</sup>) programme of the European Commission, the dimension of technical interoperability covers the technical issues of linking computer systems and services [36]. In the context of IIoT/I4.0, and concerning Internet-based services, these interactions use a common classification in four stages, viz: (1) online services, (2) online forms, (3) individual transactions, and (4) multiple transactions within integrated services. These also map to a layered architecture pattern of an information system, ranging from the presentation layer to the persistence and data layers.

The scope of our work relates to the service layer that, besides interfacing with data and presentation layers, also interfaces with a service layer of other computer systems and services, performing precisely the technical linking. To achieve interoperability among systems, technical standards facilitate the continuous exchange of data and provide the structure for moving data across the entire domain system. The applications that use standard languages take advantage of parsers and APIs that provide syntactic manipulation capabilities. SOA and mediators are the commonly used solution to ensure this linking.

The ubiquity of Internet-based technologies, based on universally open standards and specifications, has enabled a high degree of technical interoperability. The Internet is a good example, where computers and data links present data in a universally readable format simply using protocols of the TCP/IP stack.

Requirements for a good software application design follow the advantages given by the common quality attributes of a software system, concerning scalability, portability, separation of concerns. Objects mediators do not communicate directly with each other but instead communicate through the mediators. This reduces the dependencies between communicating objects enabling these quality attributes.

Implementations in the industrial domain of the mediator pattern are the basis of the IIoT, which enables to achieve technical interoperability between ground floor assets (Edge tier), and the cloud and IT infrastructure tiers (when considering an architecture pattern from reference models like IIRA). IIoT promotes the supervision of manufacturing and maintenance operations, as well as the automation of ERP production orders and logistics activities.

Industry is also moving from verticalized organizations by functions and departments to product-oriented organizations. All this points to the need for heterogeneous systems to communicate with each other. In addition, due to the technological advances, the systems are located in different places from edge to the cloud. Based on architectural decisions (Sect. 3.4), geographically distributed components or systems face the interoperability challenges in order for the processes to run properly. It should also be considered whether a system will communicate with another system at the same level or at a different level (e.g., same or different levels of ISA-95). The technological implementation of this kind of challenges in IIoT/I4.0 has been through digitization of processes and resources (i.e., digital twins), “cloudization”

of architectures, adoption of SOA/microservices and development of APIs, so that services are able to outsource functionality whenever requested by communicating through appropriate protocols.

Messaging between systems is via the implementation approach for the technical interoperability. In order to implement such messaging mechanisms, adopting relevant patterns is useful for supporting proper design decisions. In this case, enterprise integration patterns (EIP) [37] focus on implementing integration solutions based on messaging components e.g., message channels, message construction, routing, and endpoints. In terms of implementing these patterns, some middleware software products do exist in the market, thus assuring patterns adoption.

Three of the most common and industry favorite standards for IIoT at the application layer are the following:

- ISO/IEC PRF 20922 standard—commonly known as Message Queuing Telemetry Transport (MQTT)
- ISO/IEC 19464 standard—generally known as Advanced Message Queuing Protocol (AMQP)
- IETF RFC 7540 standard—widely known as Hypertext Transfer Protocol (HTTP).

These three protocols help to cover the device management for the business processes landscape. What differentiates between them are the quality attributes, which influence their own applicability in use case scenarios, or qualify restrictions on the elicitation of systems requirements. AMQP and MQTT have a publisher/subscriber architecture running over TCP, with a small message size and with reduced response time. MQTT offers low communication overheads and power consumption (lightweight protocol), and makes a good fit for simple push messaging scenarios. AMQP is designed for reliability and is more oriented to messaging. HTTP has a client/server architecture that runs over TCP/UDP protocols, enabling large message sizes, with a one-to-one data distribution and comparative higher response time.

### **IMP\_4.0 Project**

In the IMP\_4.0 project, it was necessary for the process in the cloud environment to work in the same way as in the factory shop floor. Services in the ERP (Sect. 3.4) were required to communicate with the factory shop floor, which had to perform required tasks and ensure the state of the process to be digitized at the level of cloud layer representation. In this sense, microservices must use APIs of the manufacturing systems at the factory shop floor, as well as the services themselves must provide APIs capable of receiving results from the factory floor. The scenario for this project was defined such that the information of a production order would serve as input to systems that design and specify the manufacturing operations. The project included analysis of the data structure used by the system for manipulating the cutting processes, the identification of the respective mappings for the information of the production orders, analysis of the manufacturer's APIs and subsequent specification and development of the information communication services. Technologically,

it refers to the invocation of services responsible for registering (in the manufacturing systems) the necessary information implementing the required API methods, as well as installing the middleware responsible for the communication of the service with the manufacturer system. In summary, the implementation of technical interoperability came to perceive: (1) the data structures of the systems to be integrated, (2) the ways to get information into the APIs, and (3) the adoption of AMQP as the most appropriated standard protocol for this mission in a publish/subscribe pattern.

### **UH4SP Project**

In the UH4SP project, a set of microservices (Sect. 3.4) were developed at the cloud services layer. For the middleware layer, an API gateway was installed to offer a single point of entry for a defined group of microservices, as well as the management of service endpoints of each registered factory. On the side of the industrial units, a communication process (via middleware located at the edges) was responsible for synchronizing the factory data and the respective digital twin. Technologically, the architecture included a set of microservices communicating with each other using RESTfull API, using the HTTP protocol, and using MQTT publish/subscribe pattern for synchronizing device measurements to be consumed by a business presentation layer.

### **PRODUTECH-SIF Project**

In the PRODUTECH-SIF (NPS) project, the main concern was to measure the asset efficiency (AE) of a computerized numerical control (CNC) equipment, using a product life-cycle digital thread and digital twin. The platform was called NPS (following the NPS project of the PRODUTECH-SIF program). For the management of system, devices, and actuators, an infrastructure based on an open source IIoT platform was deployed and configured. Messaging between the platform and the system, devices, and actuators used MQTT protocol. The NPS platform was used as a middleware layer between ERPs, MES and actuator devices, providing APIs that allow the systems to query the NPS platform. The NPS platform thus included an API for allowing software services to query the ontology and retrieving the outcome using RESTfull HTTP web services (cf. Sect. 3.5.2). The APIs used SPARQL queries to assure semantic interoperability between the systems (cf. Sect. 3.5.2), based on the OWL ontology aggregating ISA-95 and STEP (AP-203, AP-214), so it could generate STEP domain instructions to the asset machine, but also to promote interoperability between heterogeneous MES and ERP systems using ISA-95. As proof of concept, stress tests of the cluster were performed, which registered an average response time of 73 ms for a total of 300 simultaneous devices, publishing one value per second for each. This allowed digital twin build using near real-time data, enabling a physical system to perform real-time optimization if needed.

### 3.5.2 *Semantic Interoperability*

The semantic interoperability ensures the information sharing between services to keep the semantics flow. This concept within the IIoT setting arose from the fast increasing of entities within the smart manufacturing ecosystems. As stated by NIST SM [5], the smart manufacturing ecosystem ranges from product lifecycle, production process, and supply chain and results in a manufacturing pyramid toward vertical integration of manufacturing systems within the factory. Additionally, the horizontal integration and the end to end processes promoted by smart manufacturing and IIoT result in more entities to be included and integrated within this ecosystem. Here, integrated processes face interoperability obstacles due to lack of a unified terminology.

Despite the standardization efforts of several entities like OMG, OASIS, W3C, WfMC, ASC X12, UN/CEFACT, APICS and MESA, such broad ecosystem makes the standardization tasks very difficult due to the plethora of existing, but still growing, concepts. Some studies propose frameworks where the standards are interrelated with each other [5, 38]. However, companies are not able to implement interoperability with third-party entities if they do not properly address interoperability at the semantic level.

Addressing the semantic issue requires defining common taxonomies that are technologically addressed by defining ontologies. The ontologies can be seen as an abstraction of the data models in the context of a database. However, ontologies allow abstraction of knowledge about entities, their attributes, and their relationships, making it possible to model the domain independently of the data structure. Ontologies describe a domain at the “semantic” level as the database models describe the domain at the “real” level. Having a description at the semantic level, ontologies allow communication between different data sources. So, ontologies are used for various purposes such as defining a common vocabulary on the domain of interest to permit sharing of knowledge between different entities; enabling the reuse of the knowledge domain or providing people with an easy understanding of different domains.

A possible approach to address semantic interoperability [5] is to use an ontology as a conceptual layer for a more meaningful description of the database, providing a simpler and more efficient form of query. The ontology-based data access (OBDA) framework [39] is composed of the ontology that describes the domain: the database that stores the application data and the mapping responsible for the communication between the conceptual layer and the data layer. In the IIoT context, many current scenarios present large amounts of data available in various formats.

As previously stated in Sect. 3.2, only the PRODUTECH-SIF (NPS) project has addressed semantic interoperability. Thus, projects IMP\_4.0 and UH4SP are not discussed in this section.

## **PRODUTECH-SIF Project**

The PRODUTECH-SIF (NPS) project intends to use ontology descriptions based on STEP, namely the application protocol (AP) 238—STEP-NC [40], which allows handling of information regarding the production processes. The STEP-NC allows the modeling of necessary information about the products to be exchanged between computer aided design (CAD), computer aided engineering (CAE), computer aided manufacturing (CAM) and computerized numerical control (CNC) systems. So far, the provided ontology only implemented AP-214 and AP-203 standards, covering the geometric data of the products (CAD). Having a CAD file in STEP (AP-203 or AP-214 formats), the whole file is parsed and all instances declared in it are replicated as individuals and properties in the ontology.

Enterprises need to maintain a huge amount of legacy ERP, MES, and SCADA systems, with data in different formats (DBMS, XML, text files, etc.). The new data and new formats have to coexist with the old ones. In the PRODUTECH-SIF (NPS) scenario, the data is provided by the data model from ERP/MES, containing the business planning, logistics, and the manufacturing operations management, and CAD/CAM software with the manufacturing process management (MPM) data. Hence, the project required addressing how to integrate manufacturing process management expertise in the design and industrialization process for mechanical parts with the ERP logistic chain and manufacturing supervision process.

While interoperability between design and simulation phases of an industrialization process is currently addressed by STEP, interoperability between CAM and CNC and ERP/MES has been little addressed. Additionally, main solutions still remain proprietary. Semantic interoperability in the PRODUTECH-SIF project was addressed by OBDA architecture embedded in the IT infrastructure tier, accessible to query ERP/MES data sources (SQL Server or non-RDBMS relational databases, e.g., Excel, CSV, XML, etc.) without the specific knowledge of how they were stored in their sources.

The ontology development within the PRODUTECH-SIF (NPS) project was based on ISA-95 and ISO 10303 in order to define a vocabulary compliant with industry standards. ISA-95 was used for the concepts relating to interoperability between ERP (level 4), MES (level 3), and the shop floor systems (levels 2 and 1). The ISO 10303, informally known as STEP (Standard for Exchange of Product Data), covers a wide range of products (electronic, electromechanical, mechanical) and stages of product development (design, analysis, manufacturing).

The true interest of having a “replica” of the STEP file in an ontology is that information can be manipulated. For instance, a lot of information is present in a CAD file that can be useful to fill fields, for either the MES or ERP. Such information can be captured into the ontology. Hence, CAD files that use simple language can be transformed into ontology elements.

The first step in constructing an ontology is to define which concepts the ontology must describe. These concepts are part of the vocabulary used in the domain. In this scenario, we built into the ontology, the STEP vocabulary (AP-203, AP-214) to include the information for CAD, and the ISA-95 vocabulary for dealing with interoperability requirements and process control systems.



Besides developing an approach for defining an ontology for IIoT/II4.0 settings based on ISO 10303 and ISA-95, the project also aimed at developing a semantic interoperability platform for allowing different systems to interoperate based on the developed ontology. For addressing the semantic interoperability, the NPS platform used an open source framework for OBDA-based querying of the ontology, namely by allowing SPARQL queries to virtual RDF graphs defined by RDBMS.

The NPS platform was used within the scenarios enabled by a software component that used Java API from the open source framework. The software component allowed users accessing an OWL file relating to the ontology and another file relating to the mappings between SQL and RDF. Thus, any input data from users using SPARQL allowed querying an ontology compliant with the ISA-95 or STEP domains, and collecting the corresponding data from the MES and ERP RDBMS. This data was used in the PRODUTECH-SIF (NPS) project to instantiate a STEP-NC file template data source and use it within the vertical integration processes performed in the NPS platform (cf. Sect. 3.5.1), namely between MES and ERP systems and the shop floor.

Thus, the NPS platform was successfully implemented in a specific semantic interoperability scenario. The concept was proofed within design and manufacturing processes from planning logistic chain and manufacturing supervision process.

### 3.6 Conclusions

Requirements elicitation, architecture design and system interoperability are important dimensions of IIoT-based systems. For the requirements elicitation, the main challenge is to find the appropriate methodologies for characterizing business processes, information requirements, and hardware and software components that compose the overall ecosystem. Through experience, we have identified two alternatives for requirements elicitation in relation to the three R&D projects viz: IMP\_4.0, UH4SP, and PRODUTECH-SIF. On the one hand, the specification of UML use cases has been applied to the IMP\_4.0 project resulting in a set of low-level (also called leaf) use cases related to the ERP's modules and to the integration with cloud infrastructures. On the other hand, the UH4SP and PRODUTECH-SIF projects shared the same objective of building systems that replace and/or collaborate with existent ones. In this situation, the requirements elicitation task encompassed the definition of a set of scenarios representing key processes in a "to-be" setting. Reference models, such as the NIST CCRA and fog reference models were also used as inputs for cloud and fog computing scenarios specification within the UH4SP project.

The role of an architecture designer is to model high-level design that satisfies previously identified requirements and gives guidance for application design and development. The system architecture should identify the system's key structural elements and their relationships. For this reason, as we have already pointed out, it is necessary that the architectural design is performed first at a conceptual level at which point core design decisions must be made. The architecture design within the IMP\_4.0 project was based on the functional decomposition of requirements (using UML use

cases), whereas the 4SRS method was used to derive a logical architecture composed by the UML components that trace back to each functionality. The same approach was applied to the UH4SP project, for which a set of use cases were accordingly specified. Both exercises were the basis for generating microservices-oriented logical architectures using SoaML service participants, capabilities, service architecture, and service interfaces diagrams. On the other hand, within the PRODUTECH-SIF project, the development team defined a high-level architecture compliant to the elicited project scenario. Considering the characteristics of the scenario settings, which integrated decisions on location of legacy system components, the project used the three-tier architecture pattern for guiding the architecture design compliant with IIRA and RAMI 4.0 architectures.

In this chapter, the design dimension for technical interoperability was also addressed in the aforementioned three projects. Technical interoperability requirements were derived mainly from the need for integrating loosely coupled microservices at different tiers of the architecture. RESTfull APIs, using the HTTP protocol, and MQTT/AMQP publish/subscribe middleware have been adopted to allow communication between the relevant services.

Semantic interoperability (that is the ability of interacting systems to interpret the exchanged data to produce the required results) was addressed in the PRODUTECH-SIF project. Semantic interoperability requirements were derived mainly from the need of exchanging data between legacy components with different data models. For that, the project team developed an approach for defining an ontology for IIoT/I4.0 settings based on ISO 10303 and ISA-95 and a semantic interoperability platform for allowing different systems to interoperate based on the developed ontology.

**Acknowledgements** This work was developed within the projects IMP\_4.0: integrated management platform 4.0 (POCI-01-0247-FEDER-009147) and UH4SP: unified hub 4 smart plants (Project ID 017871), under Portuguese national grants program for R&D projects (P2020—SI IDT), COMPETE: POCI-01-0145-FEDER-007043, project “programa mobilizador PRODUTECH-SIF—Soluções para a Indústria do Futuro” under reference POCI-01-0247-FEDER-024541, co-funded by Fundo Europeu de Desenvolvimento Regional (FEDER), through Programa Operacional Competitividade e Internacionalização (POCI), and by FCT—Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2019.

## References

1. Derhamy H, Eliasson J, Delsing J (2018) Software architectural style for industrial Internet of Things. IEEE
2. Weyrich M, Ebert C (2016) Reference architectures for the Internet of Things. IEEE Softw. <https://doi.org/10.1109/MS.2016.20>
3. IIC (2017) The Industrial Internet Reference Architecture (IIRA) v1.7
4. Hankel M, Rexroth B (2015) The Reference Architectural Model Industrie 4.0 (RAMI 4.0). ZVEI
5. Lu Y, Morris KC, Frechette S (2016) Current standards landscape for smart manufacturing systems. NIST.IR.8107

6. Bohn RB, Messina J, Fang L et al (2011) NIST Cloud Computing Reference Architecture. In: IEEE World Congress on Services (SERVICES), pp 594–596
7. Lin S-W, Mellor S, Munz H, Barnstedt E (2017) Architecture Alignment and Interoperability: An Industrial Internet Consortium and Platform Industrie 4.0 Joint Whitepaper Contributors 1
8. Lu Y, Morris KC, Frechette S (2015) Standards landscape and directions for smart manufacturing systems. In: 2015 IEEE international conference on automation science and engineering (CASE), pp 998–1005
9. Infosys (2016) Interoperability Between IIC Architecture & Industry 4.0 Reference Architecture for Industrial Assets
10. Monteiro P, Carvalho M, Morais F et al (2018) Adoption of architecture reference models for industrial information management systems. In: 9th IEEE TEMS international conference on intelligent systems (IS2018)
11. Mell P, Grance T (2009) The NIST definition of cloud computing
12. Santos N, Ferreira N, Machado RJ (2017) Transition from information systems to service-oriented logical architectures: formalizing steps and rules with QVT
13. Santos N, Rodrigues H, Pereira J et al (2018) Specifying software services for fog computing architectures using recursive model transformations. In: Mahmood Z (ed) Fog computing: concepts, frameworks and technologies, 1st edn. Springer, Cham, pp 153–181
14. Fernandes JM, Machado RJ (2016) Requirements in engineering projects. Springer International Publishing, Cham
15. Varga P, Blomstedt F, Ferreira LL et al (2017) Making system of systems interoperable—the core components of the arrowhead framework. *J Netw Comput Appl* 81:85–95. <https://doi.org/10.1016/J.JNCA.2016.08.028>
16. ISA-95 (2000) ANSI/ISA-95.00.01-2000, Enterprise-control system integration part 1: models and terminology
17. Kempainen P (2016) Kempainen, Pasi. Pharma industrial internet: a reference model based on 5G public private partnership infrastructure, industrial internet consortium reference architecture and pharma industry standards. *Nord Balt J Inf Commun Technol* 2016:141–162
18. Santos N, Rodrigues H, Pereira J et al (2018) UH4SP: a software platform for integrated management of connected smart plants. In: 9th IEEE international conference on intelligent systems (IS) (in print). Funchal, Portugal
19. SCC (2013) Supply chain operations reference model (SCOR<sup>®</sup>)—revision 11.0
20. Santos N, Duarte FJ, MacHado RJ, Fernandes JM (2013) A transformation of business process models into software-executable models using MDA
21. Neiva R, Santos N, Martins JCC, Machado RJ (2015) Deriving UML logical architectures of traceability business processes based on a GS1 standard
22. Pereira A, Machado RJ, Fernandes JE et al (2014) Using the NIST reference model for refining logical architectures. In: International conference on computational science and its applications. Springer International Publishing, pp 185–199
23. Byers CC (2017) Architectural imperatives for fog computing: use cases, requirements, and architectural techniques for fog-enabled IoT networks. *IEEE Commun Mag* 55:14–20. <https://doi.org/10.1109/MCOM.2017.1600885>
24. Douglass B (1999) Doing hard time: developing real-time systems with UML, objects, frameworks, and patterns. Addison-Wesley Professional
25. OpenFog Consortium Architecture Working Group (2017) OpenFog reference architecture for fog computing
26. Jacobson I, Griss M, Jonsson P (1997) Software reuse: architecture. Process and Organization for Business Success, Addison Wesley Longman
27. Weiss DM (1999) Software product-line engineering: a family-based software development process. Addison-Wesley Professional
28. Kang KC, Kim S, Lee J et al (1998) FORM: a feature-oriented reuse method with domain-specific reference architectures. *Ann Sw Eng*
29. Bayer J, Muthig D, Göpfert B (2001) The library system product line. A Kobra case study. Fraunhofer IESE

30. Matinlassi M, Niemelä E, Dobrica L (2002) Quality-driven architecture design and quality analysis method, a revolutionary initiation approach to a product line architecture. VTT Technical Research Centre of Finland
31. Bayer J, Flege O, Knauber P (1999) PuLSE: a methodology to develop software product lines. In: Proceedings of the 1999 symposium on software reusability. ACM
32. Ferreira N, Santos N, Machado R et al (2014) A V-model approach for business process requirements elicitation in cloud design. In: Bouguettaya A, Sheng QZ, Daniel F (eds) Advanced web services. Springer, New York, pp 551–578
33. Schmidt DC, Stal M, Rohnert H, Buschmann F (2000) Pattern-oriented software architecture volume 2—patterns for concurred and networked objects. Wiley
34. Kircher M, Jain P (2004) Pattern-oriented software architecture volume 3—patterns for resource management. Wiley
35. Buschmann F, Henney K, Schmidt DC (2007) Pattern-oriented software architecture volume 4—a pattern language for distributed computing. Wiley
36. ISA2 (2017) New European Interoperability Framework (EIF)
37. Hohpe G, Woolf B (2004) Enterprise integration patterns: designing, building, and deploying messaging solutions. Addison-Wesley
38. Hannah M, Leiva C, Noller D (2018) MESA White Paper #58: The Importance of Standards in Smart Manufacturing
39. Calvanese D, De Giacomo G, Lembo D et al (2009) Ontologies and databases: The DL-Lite approach. Reasoning web 2009: reasoning web. Semantic technologies for information systems. Springer, Berlin, Heidelberg, pp 255–356
40. ISO (2003) ISO/DIS 10303-238. Industrial automation systems and integration—product data representation and exchange—part 238: application protocols: application interpreted model for computerized numerical controllers

**Part II**  
**Frameworks and Methodologies**

# Chapter 4

## Internet of Measurement Things: Toward an Architectural Framework for the Calibration Industry



**Mahdi Saeedi Nikoo, M. Cagri Kaya, Michael L. Schwartz  
and Halit Oguztuzun**

**Abstract** Many improvements have been realized in various domains, whether commercial or societal, through the use of the Internet of Things (IoT) vision, since the introduction of the IoT concept some two decades ago. Nowadays, the benefits that IoT technologies promise are becoming highly attractive for the industrial domain, in particular. There is no doubt that manufacturing of products, processing of big data produced in the production phases and gathering of customer behavior profiles, increases the efficiency of production, reduces the time to market and decreases the operational costs. This new approach that uses IoT based smart devices and intelligent sensors is called the Industrial Internet of Things (IIoT). Major global companies from various sectors such as manufacturing, automotive, mining and aviation are all taking advantage of the IIoT paradigm. The related technologies also provide limitless opportunities for the calibration industry. In turn, the world of IIoT needs to be provided with accurate and timely calibration information to increase the efficiency of processes. Having many sensitive measurement devices from customers to be calibrated by certified experts calls for networked and automated solutions. This chapter proposes an IIoT-based solution that could evolve into an architectural framework for the calibration industry.

---

M. Saeedi Nikoo · M. C. Kaya (✉) · H. Oguztuzun  
Department of Computer Engineering, Middle East Technical University, Ankara, Turkey  
e-mail: [mckaya@ceng.metu.edu.tr](mailto:mckaya@ceng.metu.edu.tr)

M. Saeedi Nikoo  
e-mail: [mahdi\\_saeedi@sparkmeasure.com](mailto:mahdi_saeedi@sparkmeasure.com)

H. Oguztuzun  
e-mail: [oguztuzn@ceng.metu.edu.tr](mailto:oguztuzn@ceng.metu.edu.tr)

M. Saeedi Nikoo  
Spark Calibration Services, Ankara, Turkey

M. L. Schwartz  
Cal Lab Solutions, Denver, CO, USA  
e-mail: [mschwartz@callabsolutions.com](mailto:mschwartz@callabsolutions.com)

**Keywords** Calibration · Electronic test equipment · Industrial Internet of Things · Industry 4.0 · Measurement · Measurement Information Infrastructure · Metrology · Architectural framework

## 4.1 Introduction

We are experiencing a new industrial revolution, sometimes referred to as Industry 4.0. By exploiting the benefits of the Internet of Things (IoT), big data, machine learning and cloud computing technologies in the industry, efficiency in production is achieved and manufacturing processes are improved [1]. This emerging approach is called the Industrial Internet of Things (IIoT). Its usage spreads to different domains wherever connected devices are used. Thus, it gives a lead to connected infrastructures to support innovative services [2]. Considering these characteristics of IIoT and related technologies, they appear promising for solving the issues in the area of calibration.

Calibration contains test and measurement devices that are manufactured with known specifications. They can lose their accuracy because of several reasons including: aging, heat, corrosion, accidental damage and so on. Furthermore, errors can be propagated to products tested with these devices. This can result in wrong decisions made, such as falsely accepting a substandard unit and mismatched parts. To ensure these devices continue functioning properly, their measurement accuracy must be verified regularly. Without proper calibration of measurement devices and without proper dissemination of calibration information, industrial automation simply could not work, since calibration is crucial for nearly all industrial applications areas.

There is a broad array of calibration disciplines such as electrical, life science and physical [3]. The focus of this chapter is on electrical devices. Electronic test equipment provides a communication interface [4] through which calibration automation can be done. Despite the fact that a big portion of calibration in industry is done manually, there have been advances in automation solutions. National Instruments (NI) LabVIEW [5] and Keysight VEE (visual engineering environment) [6] are two of the widely known examples of modern test and measurement automation platforms. They provide calibration engineers with integrated environments for developing calibration automation systems. However, these software applications typically work with local configurations of equipment at a lab setting and have less emphasis on distributed environments.

An example of a distributed automation platform for calibration automation systems is Metrology.NET<sup>®</sup> [7, 8]. This platform allows for running more than one calibration job on a single test agent. It also allows for running automation on several test agents simultaneously. The system architecture allows for distributed calibration automation management. It can be used locally in a single lab to network all the UUTs and reference equipment in the lab or it can be used across several labs where the system can manage and monitor all the units available in these labs. It

also presents a separation of concerns approach for storing test data points in a data structure separate from test procedures.

The area of calibration involves several entities. There are industrial units, equipment manufacturers, calibration labs, accreditation bodies (AB) and calibration software companies. There are also working groups that deal with calibration data in various ways either by producing or by using such data. Usually, each of these units use their own data format which results in incompatibilities in data transfers between them. Measurement information infrastructure (MII) initiative is one of the few active research groups in metrology that aims at standardizing these data types so that all the domain stakeholders use a common language of communication. Developed applications compatible with MII standards are then supposed to interact with one another. The main objective of the IoT is to provide inter-connectivity among the network of connected *things*, which leads to smarter environments. Similarly, our aim in this work is to present a framework for the application of IoT in the calibration domain. The framework is aimed to get its power through the MII.

In this chapter, we introduce the notion of “Internet of Measurement Things (IoMT)” that is inspired by the MII initiative and our experience with Metrology.NET, an MII-aware automation platform. We show how this idea can be realized by utilizing a layered IIoT architecture that separates physical equipment, cloud-based services and applications. The idea is elaborated with two proofs of concept case studies: a test point editor and a scope of accreditation editor.

In the rest of the chapter, a brief background information about IIoT along with the required background for Metrology and specifically the area of calibration including its key concepts is provided. The following section explains the shortage of automated solutions for calibration and discusses the advantages of IIoT in problem description. Related works that comprise some solutions are introduced in the same section. Metrology.NET and MII, main inspirational works for this chapter, are explained in later sections. Then, an IIoT based solution for automation and standardisation of calibration, IoMT, is elucidated through the proposed architecture. Remaining sections of the chapter provide a discussion that evaluates the suggested solution and sets some open problems and present conclusion from our study.

## 4.2 Background

In this section, a brief background of the IIoT is given. Also, the required background for the area of calibration and its terminology is provided.

### 4.2.1 Industrial Internet of Things (IIoT)

IIoT can be described as a digital environment that provides benefits of connected machines in a broad set of industrial sectors to improve productivity and reduce



time to market and costs. With respect to the Internet and the IoT, IIoT is the latest and newly emerging paradigm. Although the IoT concept and its potential have been widely known, it took some time to effectively use it in the industry. This was because of the uncertainties of how this novelty would affect the business models, value chain, workforces, productivity and products [1]. However, the advantages of using new technologies such as big data management, cloud storages and advanced machine learning techniques in the industrial context were well recognized. Some of these advantages are increased productivity, short development periods, easily developed customized products and resource efficiency [9]. Cutler [10] argues that IoT can help increase efficiency in manufacturing for many aspects including productivity, asset health, profitability, quality and safety. This branch of IIoT can be called the Internet of Manufacturing Things (IoMT).

The terms IIoT and industry 4.0 (or I4.0) are sometimes used interchangeably. Beyond the geographical effect on their usage, industry 4.0 is more common in German-speaking countries, where they have alternative meanings by indicating different focuses. Industry 4.0 is a term that is more relevant to manufacturing while IIoT is related to a wider set of concepts such as manufacturing, agriculture, health care, transportation, logistics, aviation and many more [1]. Further differences are on stakeholders, geographical focus, and representation [11]. Also, IIoT is about a technology movement whereas Industry 4.0 is more about economic concerns [12].

## ***4.2.2 Metrology and Calibration***

Metrology, originating from Greek, means the science of measurement. The International Bureau for Weights and Measures (BIPM) defines metrology as “the science of measurement, embracing both experimental and theoretical determinations at any level of uncertainty in any field of science and technology” [13]. Although it is a wide area, its main activities are defining internationally accepted units of measurement, to realise these units of measurements practically, and to apply traceability chains to establish links between measurements and reference standards. These concepts correspond to three main fields of metrology: scientific metrology, applied/technical/industrial metrology and legal metrology.

Calibration is a part of metrology. It refers to the accuracy and quality of measurements made on a particular application area using some equipment. Over time, there may be drifts in the measurement results for various reasons, such as some external factors or misuse. So, the devices must be calibrated at regular intervals to ensure they remain accurate and reliable for repeatable measurements within their lifetime. There is a margin of error in each measurement which is called “measurement uncertainty”. The purpose of the calibration is to minimize this uncertainty and to ensure that it is at an acceptable level.

Calibration ensures that systems and relevant devices are operational and reliable. Most calibration processes are carried out behind the scenes, generally without users being aware. For example, for the industries in daily life (e.g. telecommunications)

and mission-critical systems (e.g. flight safety and nuclear power plants), calibration is done regularly both for production and maintenance of the systems [13].

Calibration is critical for every domain that has a need for measurement. The confidence of the monitored and recorded data is ensured through calibration. The calibration is done by comparing the reading of equipment (or a system) with another more accurate equipment (or a system) that has been calibrated by even more accurate equipment. Also, the reference equipment itself must be directly traceable to equipment that is calibrated, based on the national standards.

Calibration is performed to determine whether there is an error on the device under test (DUT) or to verify the accuracy of the measured value. For example, calibration of a DUT thermometer can be done by measuring the temperature of the water when it is at the known boiling point. In this way, the error rate of the thermometer can be checked visually. However, determining the exact moment of the boiling point by only observing can be imprecise because it can change based on barometric pressure and purity of the water. Instead, a more accurate result can be obtained by placing a pre-calibrated reference thermometer in the water. The next step of the calibration process is to adjust the DUT to reduce the measurement error if there is a need [14].

### ***4.2.3 Calibration Domain Terminology***

Calibration has its specific terminology used by the scientific community and the industry [13, 15]. Here we give definitions for the related calibration concepts used in this work.

#### **Performance Test**

Every piece of equipment is expected to perform some specific tasks with an acceptable accuracy, based on the specified functionality specifications from its manufacturer. Electronic test equipment is accompanied with test manuals in which manufacturers provide detailed explanations on performance tests that are supposed to be performed during calibration of the equipment. These manuals provide instrument setting parameter values along with the actions to be taken step by step by the calibrator.

#### **Test Point**

Calibration mostly consists of a repeating set of steps or cycles for a set of parameters with different values for the instruments in that specific test setup. These values for parameters are provided in the test manual of the equipment. A test point refers to one of the mentioned cycles. In other words, at a specific test point, the calibrator sets a set of known parameters for the involved equipment to get a value by doing some measurement. The measured value then specifies if the test passes or fails at that specific test point.

## Measurement Uncertainty

Every measurement is subject to some uncertainty. It is a non-negative parameter that characterizes the dispersion of the values regarding a measured quantity. A measurement result is considered complete if it is accompanied by a statement of its associated uncertainty. There can be different sources for measurement uncertainty. It can come from the measuring instrument, from the item being measured, from the operator, from the environment, and from other sources. Some statistical analysis of a set of measurements and other types of information about the measurement process are used to estimate these uncertainties. There are known rules used to reach an overall estimate for uncertainty using these pieces of information. Factors such as careful calculation, traceable calibration, good record keeping, and checking can decrease measurement uncertainties [16, 17].

## Testing Terminal

One way to perform calibration of electronic test equipment is through automation software. This normally takes place at calibration lab settings. The automation software operates in a computing machine that is physically connected to test equipment that is part of the test setup. The machine responsible for this is called a testing terminal.

## Test Setup

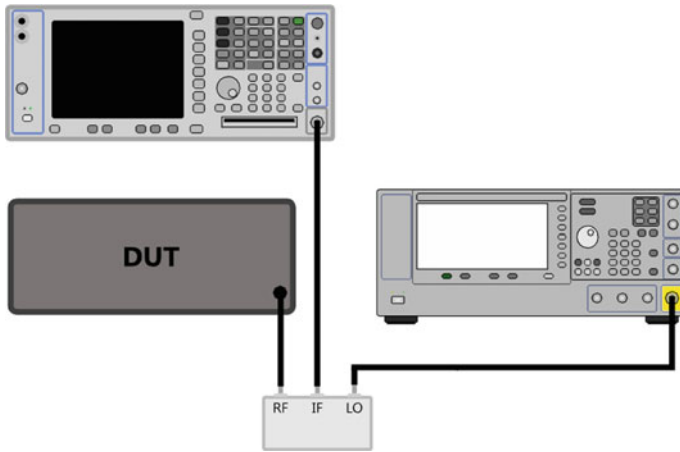
In order to calibrate a unit under test (UUT), we need to test it against a corresponding standard or reference equipment which we trust its functional accuracy. Depending on the UUT being calibrated, we may need one or more than one standard equipment. All the equipment and their physical connections to operate a specific performance test of a UUT form the test setup for that specific test. Calibration manuals provide detailed explanations on how to configure a test setup. The configuration in Fig. 4.1 shows a sample test setup with Keysight PSA and PSG reference equipment with a DUT.

## Device/Unit Under Test

The terms device under test (DUT) and unit under test (UUT) are interchangeable and used to refer to the equipment on which calibration task is to be performed. Figure 4.1 shows the DUT as a box.

## Standard Equipment

Standard or reference equipment is a piece of equipment that is functioning within acceptable limits. In other words, it is the equipment that we are sure of its functional accuracy. Reference equipment is used against device units we want to test (UUT) their functionality. For example, if we had a signal generator as UUT and we want to test it to see if it outputs correct signals, we would need a reference signal analyzer that would read the generated signal. If the read value is the same or close enough to the one generated by the signal generator, we could say that our UUT is functioning



**Fig. 4.1** A sample test setup with Keysight PSA and PSG reference equipment with DUT

properly; otherwise, we would need to adjust the signal generator to make it work properly.

### **GPIB/IEEE-488**

IEEE-488 is a digital communication bus specification. The Institute of Electrical and Electronic Engineers (IEEE) gave 488 specification number and consequently, it is sometimes referred to as IEEE-488 bus. The bus was originally named as HP-IB (Hewlett-Packard Interface Bus) as it was first introduced by HP for controlling their test equipment. Later, the test equipment arm of HP separated from the company and adopted the name Agilent. The name changed to GPIB later which is now most commonly used to refer to the bus. GPIB is the standard bus that is mostly used in calibration labs for communication between instruments. With GPIB, it is possible to connect multiple instruments to a single connector [4].

### **SCPI/IEEE-488.2**

Standard commands for programmable instruments (SCPI), which are mostly pronounced as “skippy,” is standard that defines syntax and commands to be used in controlling programmable test and measurement devices. It was defined in IEEE-488.2 specifications and originally intended to provide a common language of communication with electronic equipment, but later different equipment manufacturers started to customize parts of it. It is still the dominant language used for programming and communicating with such instruments [18, 19].

### **Types of calibration**

There are two typical ways for calibration: manual and automated. The manual way is the traditional way of calibration, which is tedious, error-prone, energy consuming and thus costly in most of the time. The same task could be done through automation

software if the equipment supports data communication with computing machines. Almost all electronic test equipment support such data communication mechanism.

There are several software systems available in the market to be used to perform testing and calibration for testing equipment. Some of these software systems such as Keysight N7800 Software TME [20] are automation systems to be used in the labs directly by technicians to run the preloaded tests on equipment while others such as Keysight VEE [6] and NI LabVIEW [5] allow domain experts to write and add their own test modules. These tools all have their own positives and limitations but the main downside that they all have in common is the difficulty of developing test scripts for technicians and even experts in the domain who do not have a programming background.

### **Scope of Accreditation**

The scope of accreditation (SoA) of a calibration lab is the official and detailed statement of the activities for which the laboratory is accredited. The formulation and assessment of the SoA encompass the main part of the accreditation process. The AB, with a degree of confidence, ensures that the laboratory qualifies for the services stated in the scope [21]. SoA serves two purposes:

- To define the specific activities of a lab which are covered by the lab's accreditation
- To provide the users of the accredited lab with a clear statement of the specific calibrations represented by the accreditation.

A laboratory's SoA is a key element of ISO/IEC 17025 [22] accreditation and an important asset to its customers. ISO/IEC 17025 is the main international standard used by testing and calibration labs.

## **4.3 Problem Definition and Related Work**

The requirement of standards and protocols, networked, and atomised applications in the calibration industry is explained in this section. Related works that have partial solutions or suggestions towards an integrated solution are also mentioned.

### ***4.3.1 Problem Definition***

Metrology, similar to many other domains, deals with a huge amount of data. There are several national institutes such as ABs, e.g., NIST (National Institute of Standards and Technology), enterprise entities such as equipment manufacturers, e.g., Keysight, calibration labs, and customers who use or produce metrology data every day. This data includes equipment specifications, measurement data, calibration lab scopes, calibration reports, and certificates. If the power of this data was harnessed appropriately, all these entities would benefit from the results.

As a result of the industrial revolution taking place in the twenty-first century, many industries are adopting several technologies such as IoT, big data, machine learning, and cloud computing. These technologies improve their business performance, thus reducing the overall cost of their business. Metrology needs to be adapted to such new technologies. In order to take advantage of these technologies, there is a need for standards to be introduced to the domain.

There is a need for solutions to apply these standards and provide an architecture to encompass all metrology data in a comprehensive way to be used by all shareholders. Our work presents such an architecture.

### 4.3.2 *Related Works*

The studies that combine metrology with the concepts of IoT have started fairly recently. One of them is conducted by Lazzari et al. [23] that discusses the term “smart metrology.” They point out that the big data collected in the industry cannot be meaningful if it is unreliable. At this point, metrology comes into play. Smart metrology is a new interpretation of metrology based on reliability. With the help of smart metrology, the calibration interval can be re-evaluated instead of regular calibrations enforced by law. Although useful notions and ideas are presented in this study, a particular solution is not proposed.

Daponte et al. present measurement applications based on IoT in a survey [24]. They classify the related work in the domains of intelligent transportation systems, smart and connected health, smart energy, smart environment, smart building, and smart factory.

Monnier discusses smart grid solutions in a white paper [25]. Although the study is not directly related to the calibration industry, it combines smart meters with IoT. In the study, the smart grid connection approaches in the literature are discussed. Then, the solutions of the author’s company to provide smarter and more connected smart grids are presented.

Angrisani et al. propose a platform based on LabVIEW for remote programming of automatic test equipment [26]. Especially when training technicians, it may not be possible to have all the necessary devices in the same lab. In such a case, it is important that a lab with the necessary devices share its resources with the other labs. This platform allows connecting to a device remotely and programming it.

Other related works were carried out in different industries. Masetti et al. use IoT-based measurement devices to monitor the wine fermentation process [27]. Tessaro et al. present a synchronization protocol with an online clock calibration method for wireless sensor networks [28]. D’Emilia et al. present a procedure for analysis of the variability causes affecting the control flow and use a mechatronic system as a case study [29]. Addabbo et al. use an IoT framework for monitoring chemical emissions in industrial plants [30]. In their work, measurement devices are used to determine the toxic gas levels.

### 4.4 Metrology.NET

The Metrology.NET automated calibration system [8] is a distributed platform for the testing and calibration process. It presents a modular approach for data management and metrology automation. It is designed to be a system of systems to bridge the gap between various types of metrology software applications currently used at calibration labs. The system follows the Lego<sup>®</sup> analogy, in which the whole system is decomposed into smaller system blocks, with a connector layer between Legos. The connector layer is supposed to join together each block of the system, which allows users to configure and build up the total solution by putting together the smaller block pieces.

Figure 4.2 depicts an overview of the Metrology.NET system and its components with the interactions among them. Metrology engineer is the one who is in charge of the server side. Testing terminal (agent) is the computer system that has direct physical interaction with UUT and standard equipment and runs the calibration process. In this example, the agent and the equipment are all connected to one another via the GPIB bus that is the most commonly used communication port for this purpose in the calibration industry.

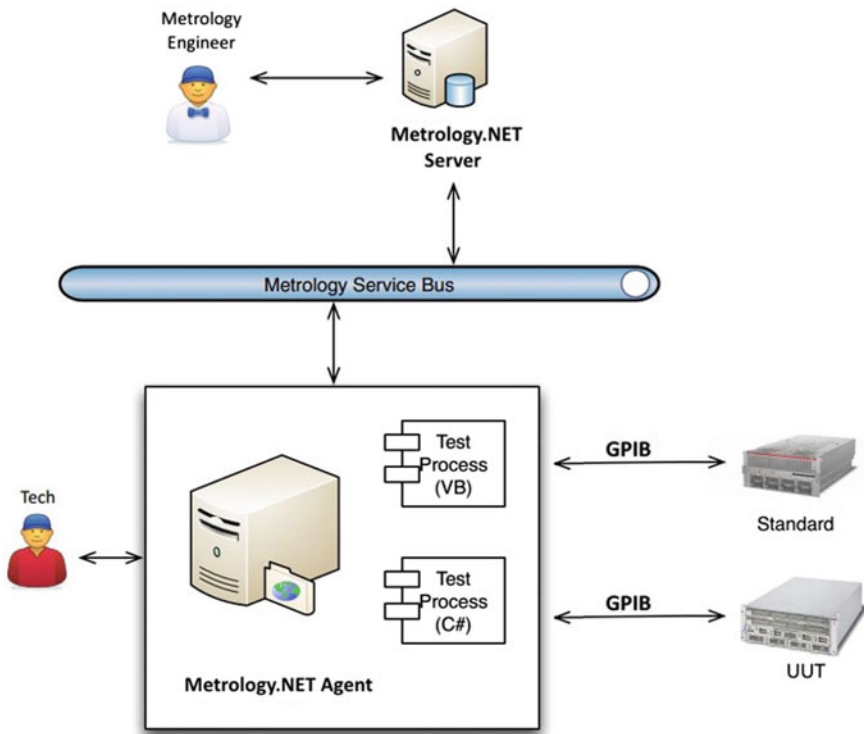


Fig. 4.2 An overview of the Metrology.NET system

The Metrology.NET platform follows a client-server architectural model. The application service of the platform is hosted by the server side. Each testing workstation is configured as a calibration agent. Technicians use either the local agents or remotely use application services to interact with the calibration process.

The server side of the platform can be physically placed in any location. It might be located locally inside a lab setting to connect to the local agents in the lab and manage their calibration tasks. Testing agents act like worker bees that do the calibration process in a collaborative way, which are all controlled through the central local server. Another option is to have a remote server for the same purpose. The remote server can have its own obvious advantages if there are no concerns related to the distance, security or other issues. The aim of the server is to hold all data related to calibration in a centralized database and provide centralized monitoring of the data and processes, which can also be used to have shared jobs and communication among different labs. Another option for the server is to deploy the server on to the cloud, which would be similar to the remote server option and also take advantage of the cloud services.

Metrology.NET seeks separation of concerns in terms of how it handles calibration data and processes. From a calibration technician perspective, a calibration job consists of a set of test points related to specific equipment. From an abstract point of view, a calibration task is the process of collecting results of a specific set of test points. Once test results are collected for all test points, calibration job can be considered complete and the system can review the collected data and certify the instrument.

Fully automated calibration increases repeatability, productivity, and accuracy in calibration labs. The aim is to provide users a high level of flexibility in the automation process. In the system, every calibration task consists of smaller reusable test modules which are developed to test specific functionalities of a UUT using specified standard equipment configuration. Subsets of test points are passed to different test modules to accomplish the automation. Each test module collects measurement results for the set of test points it receives and sends back the results up to the application server.

## 4.5 Measurement Information Infrastructure

Standards are an important part of metrology. These are measurement standards, normative standards, standard measurement practices, etc. to achieve trustworthy quality results. To remain competitive, similar to other industries, metrology requires automation and standardized interoperability to gain and improve that quality at lower costs. There is a long history of automated calibration software and the more recent laboratory management software. However, metrology covers more than calibration and workload management: Consider documentation, conformance testing, risk analysis, uncertainty analysis, service procurement, accreditation, inter-laboratory comparisons and proficiency tests, product inspections, specification use and development, etc. Here are some relevant questions:



- How many tasks have we standardized and automated and how many consume resources at every repetition?
- Why do we still maintain paper calibration certificates or their soft copies as PDF files and do manual search in accreditation scopes?
- Why don't our certificates contain full traceability chains?

Consider a set of normative standards that define data structures, taxonomies, service protocols and security for locating, communicating, and sharing measurement information. Such data standardization and protocols would eliminate ambiguity from human-readable documents, streamline many tedious and error-prone tasks, provoke new service opportunities and value streams, improve traceability, and enhance measurement quality throughout the measurement economy. Some of the benefits we would get include:

- No more tediously searching for the right instruments and service vendors
- No more manually writing, sending, interpreting documents
- No more transcribing, entering and updating information
- Our computers do it all unambiguously and automatically.

There have been different attempts and proposals on data standardization and protocols for measurement information. One of the first efforts was by the German Engineering Society (VDI) in 2006. In their document (in translation), "Format for Data Exchange in Management of Measuring and Test Equipment—Definition of Calibration Data Exchange-Format (CDE-Format)", they proposed a data exchange format for calibration domain. It seems to focus on automated calibration procurement, test equipment management, and calibration data transfer. The document describes an XML data format [31]. The document has been maintained since then and was last updated in 2012.

Fluke Calibration [32] has proposed a standard calibration data format. They claim their work is an expansion on the work done by the VDI to be used in future software packages to unify the industry and provide metrological data in an improved way. In another study, Cardoso, in her master's dissertation, proposes an information structure for calibration certificates to make it easier for calibration labs to handle certification activities [33]. The work also includes an implementation prototype in XML to represent the idea.

Mark Kuster introduced the MII concept in January 2013 in the NCSLI (National Conference of Standards Laboratories—International) Metrologist magazine in the work titled "Toward a Measurement Information Infrastructure", originally called "Metrology Information Infrastructure" [34]. In June 2017, NCSLI created the MII & Automation Committee (MII&AC) to support, develop and document the MII [35]. MII is aiming at standardizing data types in metrology. Some measurement information that can be structured includes:

- The scope of capability (SoC) or the scope of accreditation (SoA),
- Instrument spec sheets,
- Calibration and testing certificates.

It is important to note that the MII itself encompasses only open standards and infrastructure. It is the MII-aware software that brings metrology into the modern world that airline, banking, investment, online retail, and B2B industries already benefit from. It would seriously affect any business if its organization’s measurement, analysis, and management computing systems communicated this MII language with other worldwide measurement-related systems. Following are part of the MII vision [35]:

- Create a globally standardized infrastructure for creating, locating, communicating, and processing measurement information.
- Replace manually processed documents with unambiguous machine-readable data.
- Augment static web sites with smart web services.
- Open new automation horizons and empower developers to take measurement-related software to whole new levels.
- Lower the information barriers between testing & calibration labs, instrument manufacturers, vendors, ABs, and measurement consumers.

Figure 4.3 shows the measurement information flow among some of the major metrology entities. The middle layer shows the different types of metrology data that are shared among entities. The arrows represent the flow direction of the information. For example, instrument specs are provided by manufacturers to measurement consumers.

A great amount of progress has been made towards the goals of MII. Here we mention some examples. An MII SoA format was created and a search tool for it was developed. A measurement taxonomy standard is also presented by the MII group. Measurement taxonomy allows metrology systems to talk to each other. The taxon-

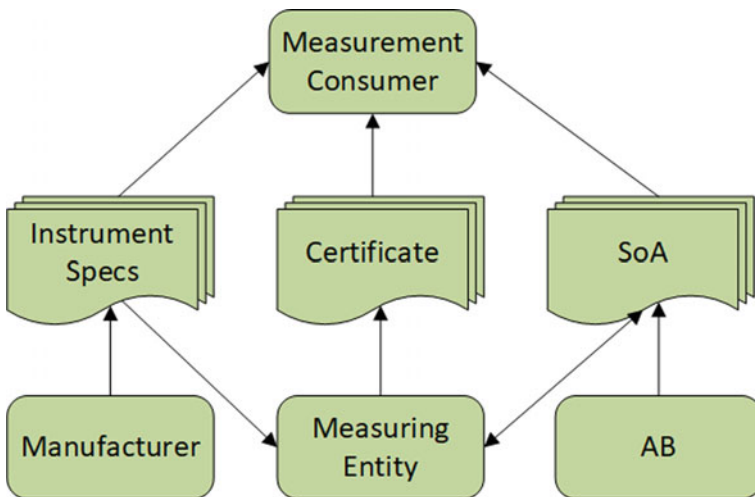


Fig. 4.3 Small excerpt from a vast network of metrology information flow

omy aims to categorize all possible measurements in different units in a hierarchical format, e.g., *Source.Volts.Sinusoidal* and *Source.Volts.DC*.

The measurement taxonomy can be applied by different MII-aware software systems such as calibration automation systems, SoA editors, and calibration lab search engines (such as Qualer search engine [36]).

### 4.6 Internet of Measurement Things (IoMT)

This section proposes a conceptual model to combine the MII and new-generation metrology software ideas with IoT. For this purpose, a layered architecture approach is adopted that contains the physical layer, the MII cloud services layer and the application layer. The proposed architecture is depicted in Fig. 4.4.

This model is derived from the reference architecture for IIoT proposed by Industrial Internet Consortium (IIC) [37], which puts forth a three-tiered architecture viz: the edge tier, the platform tier, and the enterprise tier. The edge tier is where the data collection occurs. The collected data is organized and analyzed in the platform tier

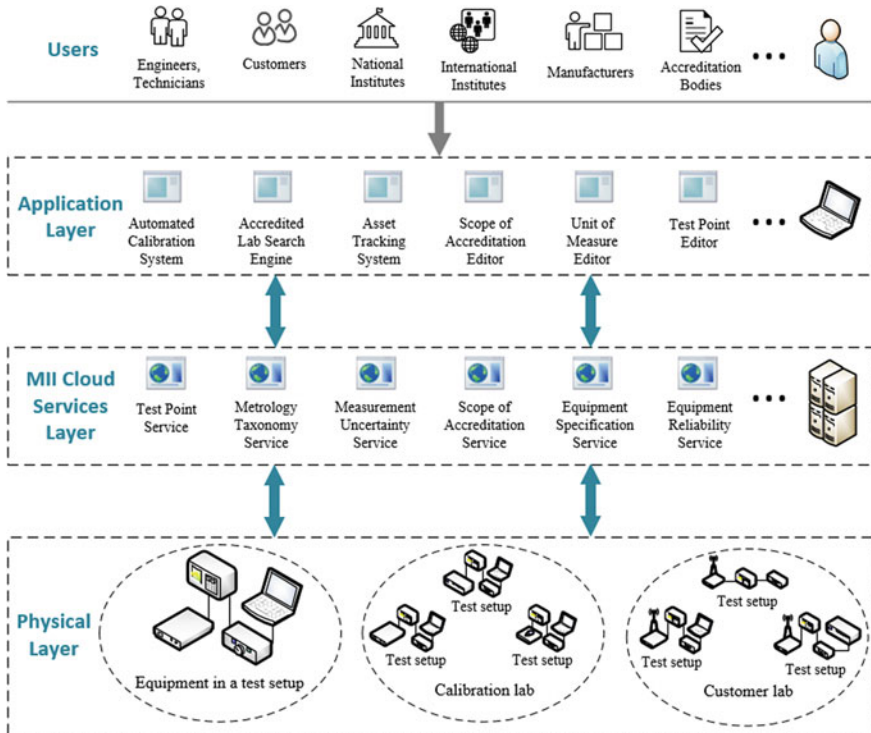


Fig. 4.4 Proposed architecture for IoMT

where services are provided. The enterprise tier is where the applications reside. In some sense, a similar architecture is used by Wan et al. [38] for software-defined IIoT in the context of Industry 4.0. Their architecture contains three layers namely physical, control, and application. Another similar layered model is provided in [24] focusing on data flow point of view. There are two layers between the topmost application layer and the lowermost physical layer; data exchange layer and information integration layer.

Zhu et al. propose an architecture to aggregate data of a certain product which is distributed to data nodes for the IIoT applications [39]. They use semantic technologies to handle the heterogeneity of the data produced by data nodes, such as various manufacturers or different stages of production that the product arrives in a supply chain. The solution proposed by the authors can be used in the calibration domain in terms of aggregating the calibration data considering scalability and efficiency. However, in this chapter, our approach aims to decrease heterogeneity by standardizing the data formats thus eliminating the need for an additional solution.

In Fig. 4.4, the physical layer of the model includes all physical equipment in the domain that are data producers. The middle layer is the MII cloud services which consists of various fine-grained services to be used by application developers of the domain. The application layer encompasses any application developed for the metrology domain. These applications share services from the lower layer. Double-headed arrows between two layers indicate the flow of data.

In the calibration industry, there are various stakeholders with different connections to the domain. These are national and international metrology institutes, ABs, equipment manufacturers, calibration labs, calibration software companies, equipment end users (customers), and probably other working units. Different user types are shown at the top of the application layer. These users can use MII services through software tools in the application layer. The arrow directed from users to the application layer indicates the “uses” relationship.

In designing the proposed IIoT architecture, we also got inspired by the Metrology.NET platform design and we plan to adopt it for IIoT. The proposed architecture and the platform are related in the following ways: The platform uses a networked architecture that is composed of several sub-systems that serve different purposes. The server side of the system has several services that are used by these sub-systems. The calibration automation system, test point editor, and measurement uncertainty calculator are examples of such sub-systems that fit into the application layer of our proposed architecture. Test point, metrology taxonomy, and measurement uncertainty calculations are examples of the services used by the platform that fit into the service layer in the proposed architecture. The physical layer of both the platform and the proposed architecture include equipment as a part of some test setup that provides the measurement data.

In spite of the similarities between the Metrology.NET platform and our proposed architecture, there are differences between the two in that the platform, with its sub-systems, works as a single software solution. Nevertheless, the proposed architecture in this chapter targets the whole domain of measurement and strongly aims at interconnectivity among different software solutions that may have commonalities or

connections in any way. In the following sub sections, we discuss the various layers and elements of the architecture.

### **4.6.1 Physical Layer**

The physical layer is made up of all the physical infrastructure of the area of calibration that produces measurement data. The framework covers the physical constituents at various scales and configurations. At the smallest scale, we can think of a single calibration setup that involves UUT and reference equipment. This is the smallest independent configuration for a calibration job. We can then scale up to a calibration lab setting, where there might be from a few to tens of calibration setups running tests simultaneously. A network of these tests setups would result in efficient lab resource management compared to the independent test setups with no interaction in-between.

In the largest scale, the physical layer encapsulates the whole domain people and organizations. We can think of all of these connected to a network. There can be intranets connecting the components within each of these units, with the Internet supplying the inter-organizational connectivity.

### **4.6.2 MII Cloud Services**

In order to encourage the different organizations in the domain to conform to the same standards and protocols when they produce a piece of data or a software system, we think there should be several robust working services based on the agreed standards and protocols. These services provide all sorts of smaller solutions that can be used in every software solution developed for the domain to create bigger solutions.

In order for these services to provide solutions for diverse applications, they should work with MII-aware data. This means the data used by these services need to be prepared in the formats defined by MII standards. The applications in the upper layer that will use these services are also supposed to comply with the MII standards.

As examples of the MII cloud services, the following services can provide the means to access the metrology data stored in the cloud to different applications on the application layer:

- Test point service: provides access to test point data in the cloud.
- Metrology taxonomy service: provides the access to the standard metrology taxonomy for all different measurement types to applications using it.
- Measurement uncertainty service: provides calculations based on different types of measurement uncertainties.
- Scope of accreditation service: provides access to calibration lab SoA data stored in the cloud.

- Equipment specification service: allows equipment manufacturers to enter their equipment specifications and provides access to this data to users such as calibration labs.
- Equipment reliability service: provides reliability analysis for measurement data stored in the cloud.

### 4.6.3 *Application Layer*

Application layer constitutes all different sorts of software that can be used by the people in the broad field of metrology. Such software could target specific groups of domain users or a broader audience. The software such as calibration automation systems are used at calibration labs, asset tracking systems can be used both by labs and customers, and SoA editors may be used by labs and ABs.

Software at the application layer may use different services from the MII cloud services layer based on the software requirements. Also, a service may be used by several applications from the application layer. For example, an automated calibration system would probably require services about test points, metrology taxonomy, uncertainty calculations and so on.

Figure 4.4 shows some examples of possible applications. Although some of them have already been implemented and are currently in use, they do not have an IIoT perspective. However, they can easily fit into the proposed architecture by using the MII cloud services and serve all kind of users in the domain. Below, brief explanations of these applications are provided:

- Automated calibration system: This application is designed for running calibration procedures in an automated way.
- Accredited lab search engine: This is a search engine for locating accredited calibration labs based on specific criteria, such as their scope parameters.
- Asset tracking system: It is used for tracking customer equipment from the point it arrives from a customer to a calibration lab until it is returned back to the customer.
- Scope of accreditation editor: This is an editor for creating documents and reports about calibration lab scope, which provides data exchange between a calibration lab and ABs.
- Unit of measure editor: It is a tool for editing and maintaining all units of measure for different types of measurements.
- Test point editor: A tool for creating and editing test point data to be used by calibration procedures.

#### 4.6.4 *Sample Scenarios*

In this section, two sample scenarios are described that represent the use of the proposed architecture in the real world. The scenarios are chosen to cover two different perspectives, in terms of information flow. One of the scenarios will consider a technical aspect of metrology and the respective information flow among metrology entities. For that, we will give the test point editor example. The other one will consider a business aspect of metrology and the related information flow for that. We will give an example scenario involving the SoA editor for this. To delineate between the current scenario and the one that can be realized based on our proposed architecture, we describe a common way of handling the job for each of the cases.

##### **The Test Point Editor Scenario**

Test points are device specific data that are provided by equipment manufacturers for calibrators to use when their equipment needs to be calibrated. Considering the current scenario, equipment manufacturers prepare calibration manuals that come with the equipment for customers. Test point data are part of these manuals. An important feature of these manuals is that they are written to be read by humans and are not machine-readable. As there is no standard data format, each manufacturer develops its own way of preparing these data. Consequently, the lack of such standards usually results in a great amount of variation in how they are formatted.

In the case of manual calibration, calibration lab technicians must read and follow the calibration manuals containing these data to perform the calibration job. However, in case of automation, there are usually two possibilities: Either labs use off-the-shelf software or they write their own calibration automation software. In the first case, they would not deal with test point data as they are already in the software. In the second case, however, they need to translate the data provided by manufacturers to machine-readable data to be used in their automation. Such a translation usually requires a great amount of time and effort for them as they need to understand and translate such data to computable data.

Now we explain how diverse components from layers of the architecture may collaborate to make it possible for test point data to be handled in a better way. Considering the proposed architecture, we can think of such a scenario: Manufacturers—as the entities responsible for the creation of test points, would use a test point editor to store these data for a newly introduced equipment. This data would be stored in the cloud to be used by them and other entity users. The test point editor would use *test point* and *metrology taxonomy* services and probably some other services. Calibration labs are the main users of test points as they use these data in the calibration process. These labs would use test point editor with a different interface or role to access such data. Since the test point is central to calibration, there might be other software systems in the application layer that will use *test point* service. Calibration automation software is an example of such systems. They would also use the service to access test point data stored in the cloud. All the data follow a standard format, the service(s) provides access based on that specific format, different applications use

the same service(s) to write or retrieve the data. Thus, we achieve interoperability and data sharing among related entities.

### **The SoA Editor Scenario**

We first consider the current steps for a calibration lab to get accredited for their capabilities. As a first step, metrology engineers at a calibration lab need to perform the uncertainty calculations for all measurements they take at the lab. The calculations are normally done using a spreadsheet tool. Next, they create a document regarding these calculations and submit this document to a national AB. After that, the AB experts analyze this document and do a thorough on-site analysis of the lab. In the end, the AB officials get back to the lab with the certificate of accreditation and publish the lab scope on their website in a free format. The information regarding accredited capabilities is completely disconnected from the original uncertainty calculations and the daily calibration product. Customers who want to get their equipment calibrated are not able to easily find a calibration lab that is best for their needs.

Based on our proposed architecture, we explain now how relevant software from the application layer, using services from the MII services layer provide solutions for various problems regarding SoA requirements. The MII group has already proposed an SoA data format to the community [40]. This data format captures all data used to cover various aspects of SoA for calibration labs. All SoA data would be stored in the cloud and there would be services in the MII services layer to provide access to such data. One or more applications from the application layer would provide user groups with interfaces to access these data. Lab capabilities would firstly be created by calibration labs and uploaded to the cloud using the SoA editor. If a lab wants to apply for accreditation, access to the lab's scope data would be provided to the AB. Then the AB can reach the lab data from the cloud, through the SoA editor. If the capabilities get approved by AB experts, the lab becomes formally accredited and a certificate is generated by the tool for the lab, and the lab scope data would be preserved in the cloud. Now customers who want to get their equipment calibrated can use other applications such as accredited lab search tool from the application layer to look for different accredited labs with diverse capacities and choose the one that best suits their needs. Such a search application would use the SoA service and some other services from the MII services layer to access the SoA data stored in the cloud.

## **4.7 Discussion**

Despite its promise, the MII initiative is not quite mature. To reach maturity, common services of the area of calibration, e.g., services in the middle layer of the proposed conceptual model should be implemented. Making these services globally available is important. Also, building applications through basic graphical interfaces (such



as drag and drop manner) will ease the development process by non-programmers. Therefore, realizing MII can help the calibration industry to reap the benefits of IIoT.

Having standardized data formats and common services would be the ideal case. However, adoption of these concepts by the industry may take a while. One reason is that the calibration industry is worldwide and has many vendors, customers, calibration labs, and accreditation bodies with their own characteristics.

The presented architecture is looking at the domain from the functional point of view. There are also some nonfunctional concerns that need to be considered. Some of the main concerns are confidentiality, reliability, traceability/provenance, governance/community process, and usability. For the architecture to gain attention and popularity, there is a need for these concerns to be researched and addressed appropriately.

## 4.8 Conclusion

This chapter envisions how the calibration industry and IoT technologies come together. In this sense, promising ongoing works to achieve this goal, namely, the MII initiative and the Metrology.NET platform, are discussed. Inspired by these two approaches, a conceptual architecture is proposed to introduce IIoT to the calibration industry. This model assumes the use of the standards of the MII initiative by the stakeholders in the calibration. The common services are provided by cloud servers and application developers can readily use them to build their software.

The proposed framework, or some alternative thereof, should be implemented in the future. Although some of the applications in the application layer are already implemented and used locally by some labs, they are limited in terms of allowing data exchange by the metrology community. After porting existing applications to web services, new services should be added to appeal to more stakeholders. Moreover, MII itself needs to keep evolving to address ongoing technological advances and raised expectations of stakeholders.

**Acknowledgements** We would like to thank Mark Kuster for his insightful remarks on the first draft of this chapter.

## References

1. Gilchrist A (2016) Industry 4.0: The Industrial Internet of Things. Apress
2. Sisinni E, Saifullah A, Han S, Jennehag U, Gidlund M (2018) Industrial Internet of Things: challenges, opportunities, and directions. *IEEE Trans Ind Inf* 14(11):4724–4734. <https://doi.org/10.1109/tii.2018.2852491>
3. Czichos H, Saito T, Smith LE (eds) (2011) Springer handbook of metrology and testing. Springer Science & Business Media

4. IEEE Standard Digital Interface for Programmable Instrumentation (1987) Institute of Electrical and Electronics Engineers, ISBN 0-471-62222-2. ANSI/IEEE Std 488.1(1-1987):iii
5. National Instruments (2019) What is LabVIEW? <https://www.ni.com/labview>. Accessed Jan 2019
6. Keysight Technologies (2019) VEE Pro 9.33. <https://www.keysight.com/en/pd-1476554-pn-W4000D/vee-pro-932?cc=US&lc=eng>. Accessed Jan 2019
7. Metrology.NET Calibration Automation Platform (2019) <https://www.metrology.net/>. Accessed Jan 2019
8. Cal Lab Solutions Inc. (2019) <http://www.callabsolutions.com/>. Accessed Jan 2019
9. Lasi H, Fettke P, Kemper HG, Feld T, Hoffmann M (2014) Industry 4.0. *Bus Inf Syst Eng* 6(4):239–242
10. Cutler TR (2014) The internet of manufacturing things. *Ind Eng* 46(8):37–41
11. Bledowski K (2015) The internet of things: Industrie 4.0 vs. the industrial internet. <https://www.mapi.net/forecasts-data/internet-things-industrie-40-vs-industrial-internet>. Accessed Jan 2019
12. Jeschke S, Brecher C, Meisen T, Özdemir D, Eschert T (2017) Industrial internet of things and cyber manufacturing systems. In: Jeschke S, Brecher C, Song H, Rawat D (eds) *Industrial internet of things*. Springer Series in Wireless Technology, Springer, Cham
13. Joint Committee for Guides in Metrology (2012) International vocabulary of metrology—basic and general concepts and associated terms (VIM), 3rd edn. [https://www.bipm.org/utills/common/documents/jcgm/JCGM\\_200\\_2012.pdf](https://www.bipm.org/utills/common/documents/jcgm/JCGM_200_2012.pdf). Accessed Jan 2018
14. Fluke Calibration (2019) About calibration. <https://us.flukecal.com/literature/about-calibration>. Accessed Jan 2019
15. Bucher JL (2012) *The metrology handbook*, 2nd edn. ASQ Quality Press
16. Howarth P, Redgrave F (2008) *Metrology—in short* 3rd edition. EURAMET project 1011, July 2008
17. Bell S (2001) Measurement good practice guide no. 11 (issue 2). A beginner’s guide to uncertainty of measurement. National Physical Laboratory, Teddington, Middlesex, United Kingdom
18. SCPI Consortium (1999) Standard commands for programmable instruments. <http://www.ivifoundation.org/docs/scpi-99.pdf>. Accessed Jan 2019
19. Standard Digital Interface for Programmable Instrumentation—Part 2: Codes, formats, protocols and common commands (Adoption of (IEEE Std 488.2-1992) (2004) IEEE 488.2 IEC 60488-2 First edition 2004–05
20. Keysight Technologies (2009) The TME tutorial. [https://www.keysight.com/upload/cmc\\_upload/All/TMETutorial\\_E\\_02\\_11.pdf](https://www.keysight.com/upload/cmc_upload/All/TMETutorial_E_02_11.pdf). Accessed Jan 2019
21. International Laboratory Accreditation Cooperation (2010) Guideline for the formulation of scopes of accreditation for laboratories ILAC-G18:04/2010
22. International Organization for Standardization (2019) ISO/IEC 17025—testing and calibration laboratories. <https://www.iso.org/home/standards/popular-standards/isoiec-17025-testing-and-calibra.html>. Accessed Jan 2019
23. Lazzari A, Pou JM, Dubois C, Leblond L (2017) Smart metrology: the importance of metrology of decisions in the big data era. *IEEE Instrum Meas Mag* 20(6):22–29
24. Daponte P, Lamonaca F, Picariello F, De Vito L, Mazzilli G, Tudosa I (2018) A survey of measurement applications based on IoT. In: *Proceeding workshop on metrology for Industry 4.0 and IoT*. Brescia, Italy, April 16–18
25. Monnier O (2013) A smarter grid with the Internet of Things. Texas Instruments, October 2013
26. Angrisani L, Cesaro U, D’Arco M, Grillo D, Tocchi A IOT enabling measurement applications in Industry 4.0: platform for remote programming ATES. In: *Proceeding workshop on metrology for Industry 4.0 and IoT*. Brescia, Italy, April 16–18
27. Masetti G, Marazzi F, Di Cecilia L, Rovati L (2018) IOT-based measurement system for wine industry. In: *Proceeding workshop on metrology for Industry 4.0 and IoT*. Brescia, Italy, April 16–18
28. Tessaro L, Raffaldi C, Rossi M, Brunelli D (2018) Lightweight synchronization algorithm with self-calibration for industrial LORA sensor networks. In: *Proceeding workshop on metrology for Industry 4.0 and IoT*. Brescia, Italy, April 16–18

29. D'Emilia G, Gaspari A, Natale E (2018) Measurements for smart manufacturing in an Industry 4.0 scenario. A case-study on a mechatronic system. In: Proceeding workshop on metrology for Industry 4.0 and IoT. Brescia, Italy, April 16–18
30. Addabbo T, Fort A, Mugnaini M, Parri L, Parrino S, Pozzebon A, Vignoli V (2018) An IoT framework for the pervasive monitoring of chemical emissions in industrial plants. In: Proc workshop on metrology for Industry 4.0 and IoT. Brescia, Italy, April 16–18
31. VDI/VDE 2623 (2012) Format for data exchange in management of measuring and test equipment—Definition of Calibration Data Exchange-Format (CDE-Format). <https://standards.globalspec.com/std/9913432/vdi-vde-2623>. Accessed Jan 2019
32. Johnston M (2018) A proposal for a standard calibration data format. <https://eu.flukecal.com/fr/blog/proposal-standard-calibration-data-format>. Accessed Jan 2019
33. Cardoso AMR (2018) Sistema de informação para troca de certificados de calibração digitais. Master dissertation, University of Porto
34. Kuster M (2013) Toward a metrology information infrastructure. Metrologist NCSLI Worldwide News, Jan 2013
35. MII (2019) MII Initiative Knowledge Base. <http://miiknowledge.wikidot.com/>. Accessed Jan 2019
36. Qualer (2019) Introducing Qualer Search. [https://qualer.com/qualer\\_search/](https://qualer.com/qualer_search/). Accessed Jan 2019
37. Lin SW, Miller B, Durand J, Bleakley G, Chigani A, Martin R, Crawford M (2017) The Industrial Internet of Things, Volume G1: Reference Architecture. Industrial Internet Consortium, January 2017
38. Wan J, Tang S, Shu Z, Li D, Wang S, Imran M, Vasilakos AV (2016) Software-defined industrial internet of things in the context of industry 4.0. *IEEE Sens J* 16(20):7373–7380
39. Zhu T, Dhelim S, Zhou Z, Yang S, Ning H (2017) An architecture for aggregating information from distributed data nodes for industrial internet of things. *Comput Electr Eng* 58:337–349
40. Zajac D (2016) Creating a standardized schema for representing ISO/IEC 17025 scope of accreditations in XML data. In: NCSL international workshop & symposium. Saint Paul, MN, July 24–28

# Chapter 5

## Architecture Modeling of Industrial IoT Systems Using Data Distribution Service UML Profile



Bedir Tekinerdogan, Turgay Çelik and Ömer Köksal

**Abstract** The adoption of Internet of Things (IoT) in the industrial sector, that is the IIoT, has led to a dramatic increase in the volume of data that is usually distributed over multiple devices. To realize the distributed execution and management of IIoT systems, various requirements and quality factors must be satisfied. To reduce the effort for developing IIoT-based systems, a middleware seems to be a feasible solution. A middleware that is directly related to data-intensive systems in which quality of service parameters are explicitly considered is the Data Distribution Service (DDS) software. The DDS has been applied for the development of high-performance distributed systems such as in the defense, finance, automotive, and simulation domains. Yet, for modeling the DDS-based IIoT systems, the specific modeling abstractions are missing which impedes the overall design. To overcome this problem, we provide a UML DDS profile that can be used for modeling the architecture of DDS-based IIoT systems. Along with the profile, we propose a systematic method for applying the profile. We illustrate the application of the profile for modeling the architecture of a smart traffic system.

**Keywords** Industrial internet of things · IIoT · Data distribution service · DDS · Software architecture analysis · Design optimization · Model-driven development · UML

---

B. Tekinerdogan (✉)  
Wageningen University, Wageningen, The Netherlands  
e-mail: [bedir.tekinerdogan@wur.nl](mailto:bedir.tekinerdogan@wur.nl)

T. Çelik  
MilSOFT Software Technologies, Ankara, Turkey  
e-mail: [tcelik@milsoft.com.tr](mailto:tcelik@milsoft.com.tr)

Ö. Köksal  
ASELSAN Research Center, Ankara, Turkey  
e-mail: [köksal@aselsan.com.tr](mailto:köksal@aselsan.com.tr)

## 5.1 Introduction

The adoption of Internet of Things (IoT) in the industrial sector, that is the IIoT, has led to a dramatic increase in the volume of data that is usually distributed over multiple devices. To realize the distributed execution and management of IIoT systems, various requirements and quality factors must be satisfied. In general, a distributed system consists of multiple software components that are located on networked computers, but act and run as a single system. The computers that are in a distributed system can be connected by a local network and be physically close to each other or they can be connected in a wide area network and geographically distant. Distributed systems offer many benefits over centralized systems, including scalability, concurrency, and redundancy.

To reduce the effort for developing distributed systems, common middleware architectures have been introduced. The middleware provides common services such as name and directory services, discovery, data exchange, synchronization, and transaction services [6]. The publish–subscribe middleware adopts an event-driven approach based on publish–subscribe communication pattern. This pattern has gained broad attention in the development of loosely coupled, scalable large-scale applications. One of the important and popular publish–subscribe middleware is the Data Distribution Service (DDS) for real-time systems, which has been defined by the Object Management Group (OMG) to provide a standard data-centric publish–subscribe specification for distributed systems. DDS has been applied for the development of high-performance distributed systems such as in the defense, finance, automotive, and simulation domains [7].

In this chapter, we focus on the adoption of middleware for IIoT-based systems. Such systems are typically characterized by their data-intensive and asynchronous behavior in which the quality of service parameters needs to be carefully defined. A middleware that is directly related to data-intensive systems in which quality of service parameters is explicitly considered is the Data Distribution Service (DDS) middleware. A DDS-based system usually consists of multiple participant applications each of which has different responsibilities in the system. These participants can be allocated in different ways to the available resources, which leads to different configuration alternatives. Usually, each configuration alternative will perform differently with respect to the execution and communication cost of the overall system. In general, the deployment configuration is selected manually which is suitable for small to medium-scale applications, but for larger applications, this is not tractable. The OMG DDS specification does not provide an explicit approach to guide the distribution and allocation of the participants to optimize the deployment configuration with respect to performance. The deployment configuration is usually selected manually, which is suitable for small to medium-scale applications, but gets intractable when larger applications are considered.

In this chapter, we describe the realization of a DDS UML profile that we have extended to support the generation of feasible deployment alternatives. The design is used to define alternative execution configurations that refine the number and parameters of the corresponding design elements. Based on the application design and the

execution configuration, the feasible deployment alternatives can be algorithmically derived. The presented approach is supported by corresponding tools that support the application design, the execution configuration definition, and the automatic generation of feasible deployment alternatives using model-driven development techniques. We illustrate the approach for modeling a smart city parking system.

The remainder of the chapter is organized as follows. In Sect. 5.2, we provide the background on publish–subscribe systems, and in Sect. 5.3 on DDS. Section 5.4 defines the case study that will be used in subsequent sections. Section 5.5 describes the presented DDS UML profile. Section 5.6 discusses the architecture modeling approach using the provided profile. Section 5.7 presents the related work, and finally, Sect. 5.8 concludes the chapter.

## 5.2 Publish–Subscribe Architecture

As stated before, current IIoT-based systems are typically characterized by their data-intensive and asynchronous behavior. For this purpose, the so-called publish–subscribe architecture pattern can be adopted. The architecture defines the higher-level structure of the system that has a direct impact on the other development artefacts [16]. A pattern is a generic solution structure to recurring problems. The publish–subscribe pattern is one of the key architecture design patterns [1] and has been used in several different standard infrastructures such as the Java Message Service (JMS) [12], Data Distribution Service (DDS) [11], Distributed Interactive Simulation (DIS) [2], and high-level architecture (HLA) [3]. Although the publish–subscribe pattern has been applied in several applications and infrastructures, we can still define the general reference architecture as shown in Fig. 5.1 [18–20].

A typical publish–subscribe system consists of a group of participants which are deployed on a number of application nodes. Each participant defines a number of publisher and subscribers that read/write data objects and events. Data objects and events are elements of data exchange model of the publish–subscribe system.

Although the current publish–subscribe middleware systems share common features, we can also identify differences. The common and variant features can be expressed using a feature diagram as shown in Fig. 5.2 and which has been derived from our earlier study [19].

Publish–subscribe middleware systems can be distinguished based on the type and the service model. Regarding the type, we can identify data-centric, message-centric, or object-centric approaches as follows:

- In the message-centric approach, the middleware is not aware of the content of the data; it is just responsible for transmitting the messages among participants.
- In data-centric approach, the middleware is aware of the content and can impose quality of service parameter values on the data.
- In object-centric approaches, the middleware is responsible for transmitting objects among participants.

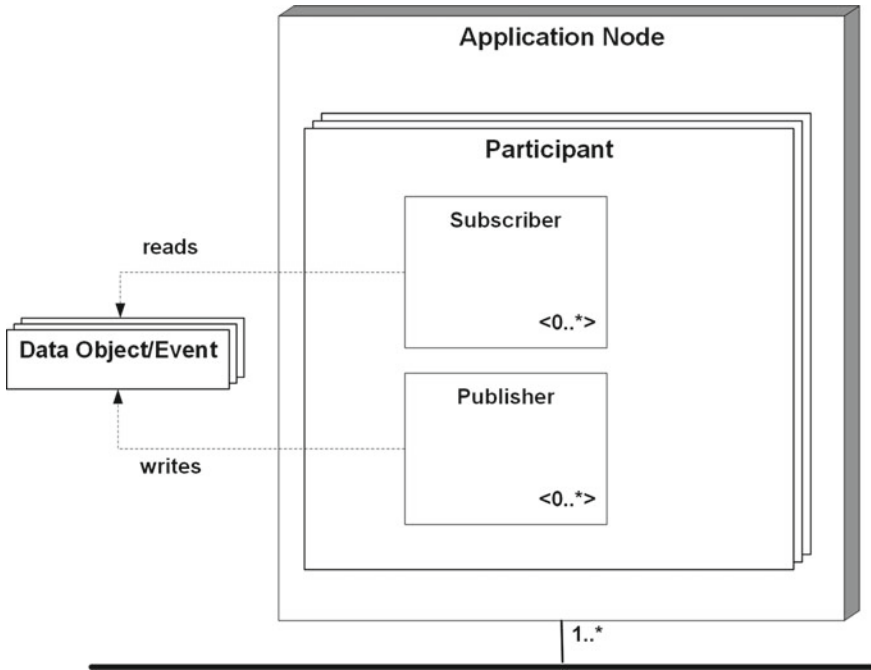


Fig. 5.1 Reference architecture for publish-subscribe systems

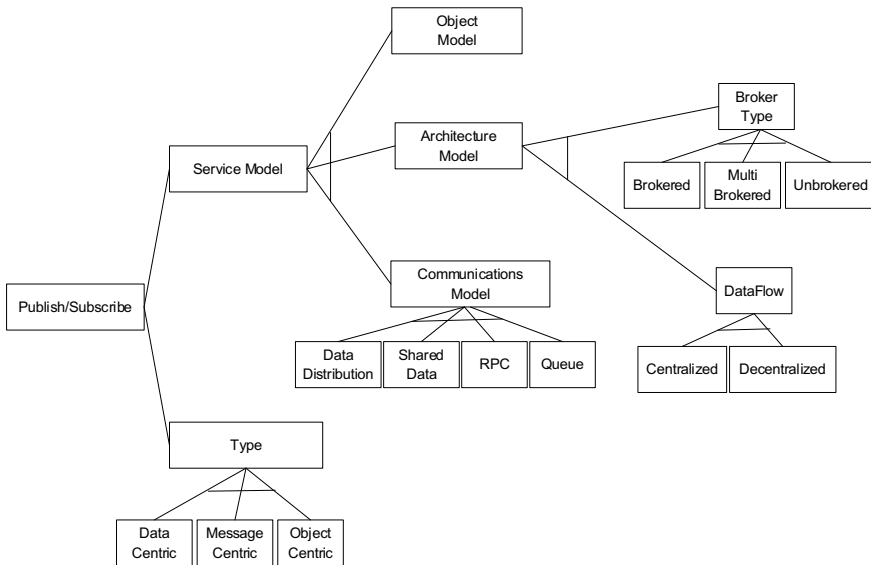


Fig. 5.2 Feature model of publish-subscribe systems (adapted from [19])

**Table 5.1** Publish–subscribe middleware approaches

Pub/subtechnique	Type	Pub/subtechnique	Type
DDS	Data centric	Data distribution	Decentralized/unbrokered
HLA	Data centric	Data distribution	Decentralized/unbrokered or brokered
DIS	Data centric	Data distribution	Decentralized/unbrokered
TENA	Data centric	Data distribution	Decentralized/unbrokered
JMS	Message centric	Queue based	Centralized/brokered or centralized/multibrokered
CORBA event services	Object centric	Remote procedure call	Centralized/multibrokered

The service model of a publish–subscribe middleware can be characterized based on: (1) communications model, (2) architecture model, and (3) object model. Communication model defines communication approach that is applied by the participants. The communication approach, in turn, can be based on data distribution, shared data, queuing, and remote procedure call. The architecture model of a middleware can be either centralized or decentralized denoting whether the data flows through a central unit or not. Further, the architecture model can include a broker that manages the data flow. The architecture can be unbrokered, i.e., there is no broker defined or multibrokered, whereby multiple brokers manage the data flow. The final distinguishing character of the service model is the adopted object model that defines the type of middleware entities that is adopted in the interaction among participants.

Based on the feature diagram (Fig. 5.2), we can instantiate different publish–subscribe systems. In Table 5.1, we list the publish–subscribe systems that we can identify in the literature. These include DDS, HLA, DIS, and TENA and CORBA Event Services. For further details about the comparison of these publish–subscribe approaches, we refer to [18–20].

### 5.3 Data Distribution Service (DDS) Middleware

In this section, we describe the background for understanding and supporting the approach that we present in this chapter. Detailed information on DDS can be found in [4, 8, 10, 13]. Based on these studies, Fig. 5.3 shows the conceptual model for the DDS specification that is adapted from the DDS specification [9].

The concepts in the DDS specification are defined as follows:

- *Domain* is a logical concept which represents the set of applications that can communicate with each other.
- Within the same DDS system, multiple *Domains* can be defined indicating different sets of applications that communicate with each other.



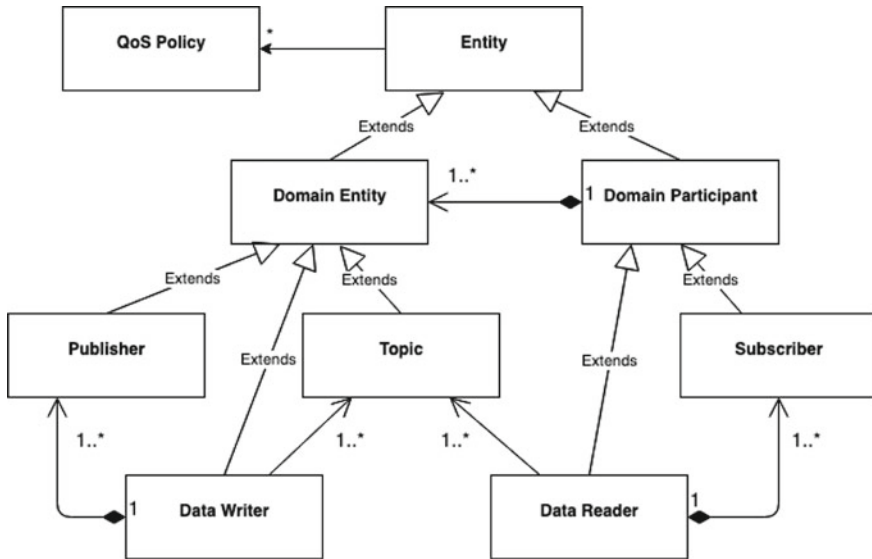


Fig. 5.3 Reference architecture for DDS-based systems (adapted from [9])

- A *Domain* includes one or more *Domain Participants* which represent the local membership of the application in the corresponding domain.
- *Domain Participant* may participate in more than one domain at the same time.
- Each *Domain Participant* may include one *Publisher* and one *Subscriber*.
- *Publisher* represents the objects responsible for data production and updates.
- A *Publisher* includes one or more *Data Writers* that publish data of different data types.
- *Subscriber* is responsible for receiving published data and making it available to the participant.
- A *Subscriber* includes one or more *Data Readers* to access published data in a type-safe manner.
- The communication between *Data Readers* and *Data Writers* is established via *Topics*.
- A *Topic* defines a unique name, data type, and a set of quality services to the published/subscribed data.
- DDS provides the ability to attach *Quality of Service (QoS)* parameters to all these entities in order to specify the behavior of a service. Examples of these QoS parameters are the data reliability, latency cost, how long the data is valid, etc.
- Applications communicate with each other based on topics. Communication between applications can only be realized only if the topic names and the defined QoS parameters match.

The conceptual model of Fig. 5.3 defines the so-called data-centric publish–subscribe (DCPS) part of the DDS specification which is mandatory for DDS implementations. In addition to DCPS, the DDS specification also defines the data local

reconstruction layer (DLRL) which is an optional layer that may be built on top of the DCPS layer. The purpose of the DLRL is to provide a seamless integration with object-oriented language constructs. For further details about these specifications, we refer to OMG DDS Specifications [9].

### 5.4 Case Study

In this section, we define a case study that will be used to illustrate the problem statement and the approach in further sections. The case study is within the context of smart city engineering and includes smart traffic system (STS). The high-level reference architecture of STS is depicted in Fig. 5.4. STS consists primarily of sensors and vehicles. Sensors are the devices that monitor the environment and provide the corresponding data. Vehicles use the sensor data and publish their position and other relevant information to the STS. Within the case study, we distinguish between the following sensor types: traffic light, incident detector, congestion detector, speed camera, parking detection sensor, bicycle station, parking lot, and weather sensor. Vehicles can be of the following types: car, truck, ambulance, taxi, bicycle, and bus. The sensors and control units are thin clients which do not contain any business logic. In this case, all the STS elements can communicate with the STS.

STS is, in essence, a data-intensive system with stringent demands for QoS parameters. As stated before, the OMG DDS middleware explicitly considers QoS properties and as such is very suitable to realize the STS system. In order to implement STS using DDS, we need to map the application domain (smart city) concepts to the DDS concepts viz: domain, domain participants, publishers, subscribers, and the topics in the STS case study. The DDS concept within the smart city domain is traffic domain. Domain participants might be grouped as vehicles, sensors, and managers. Vehicles and sensors are the virtual entities of the corresponding physical entities as we have described above. Managers define the domain participants that include the communication and business logic necessary for executing the required services. As stated before, each domain participant can have zero or one publisher and zero or one subscriber.

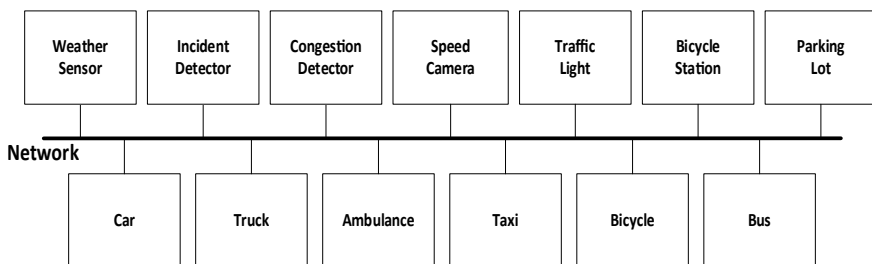


Fig. 5.4 High-level reference architecture of the smart city case study

## 5.5 Data Distribution Service UML Profile

To support the analysis and design of object-oriented systems using DDS technology, the OMG has specified the Universal Modeling Language (UML) profile for Data Distribution Specification [8]. The profile enables definition of all DDS artefacts defined in the reference architecture as given in Fig. 5.5. This profile also enables the definition of DDS data types which topics will be built on. The profile separates DDS artefacts in three packages including data-centric publish–subscribe (DCPS), data local reconstruction layer (DLRL), and DDS Common.

The DCPS defines the mandatory part of the DDS specification used to provide the functionality required for an application to publish and subscribe to the values of data objects. As stated before, the DLRL is the optional portion of the DDS specification used to provide the functionality required for an application for direct access to data exchanged at the DCPS layer. The DDS common package defines the distributed data communications specification that allows quality of service (QoS) policies to be specified for data timeliness and reliability. DDS UML profile is independent of implementation languages. The dependencies between the packages are shown in Fig. 5.5.

Figure 5.5 indicates that the DCPS and DLRL packages depend on DDS common. Several tools that implement the draft specification of the above UML profile for Data Distribution Specification are already available and ready to be used (e.g., enterprise architect [14]).

We realized the OMG DDS UML profile in the Eclipse Graphical Modeling Framework (GMF) [15]. Eclipse GMF uses the Eclipse Modeling Framework (EMF) as metamodeling infrastructure. We modeled OMG DDS UML profile metamodel in EMF environment. For the sake of modularity and understandability, we divided the profile to submetamodels that together form the OMG DDS UML profile.

The metamodel for the common package is illustrated in Fig. 5.6. All other classes are derived from these basic artefacts. Hereby, entity defines an abstract class, specialized by all entities defined in the metamodel. Specification defines a container of properties and a constraint on the range of values represented by a typed element.

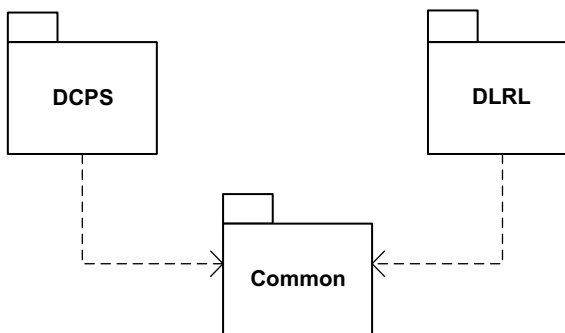


Fig. 5.5 OMG UML profile for data distribution specification top-level packages

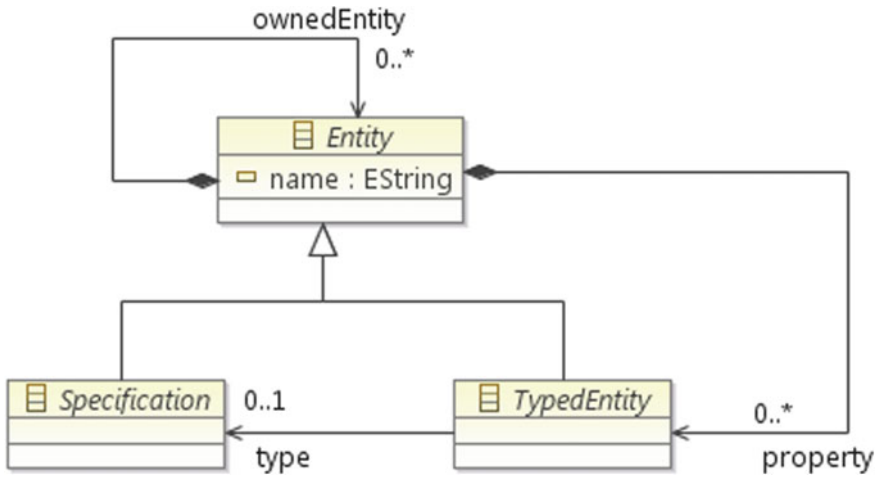


Fig. 5.6 Metamodel for DDS UML profile/common/core package

Finally, typed entity defines an entity that has a type that serves as a constraint on the range of values the entity can represent.

Our modeling tool realizes the necessary parts of the UML profile for Data Distribution Specification to define the DDS types, the DDS topics, the domain participants, and the publish–subscribe relations. The relationships among domain, domain participant, publisher, subscriber, data reader, and data writer artefacts are shown in Fig. 5.7.

All entities in Fig. 5.7 extend a common parent class that is called the “DomainEntity.” OMG DDS defines a set of quality of services (QoS) that can be associated with different domain entities (Fig. 5.8).

Domain participants publish and subscribe “Topics.” The high-level metamodel for topics is given in Fig. 5.9. Topics consist of topic fields.

The metamodel for topic fields is shown in Fig. 5.10. DDS enables associating different QoS policies with topics and other domain entities at different levels such as publishers, data readers, etc. We modeled the relations between domain entities and QoS policies. For example, association of topic with applicable QoS policies is given in Fig. 5.11. Finally, we also modeled all QoS policies as given in Fig. 5.12. With the described models, we have provided a DDS UML profile that can be used to design DDS-based IIoT systems.

## 5.6 Architecture Modeling Approach

In this section, we provide a systematic process for defining a DDS-based distributed system. The approach is represented in Fig. 5.13.

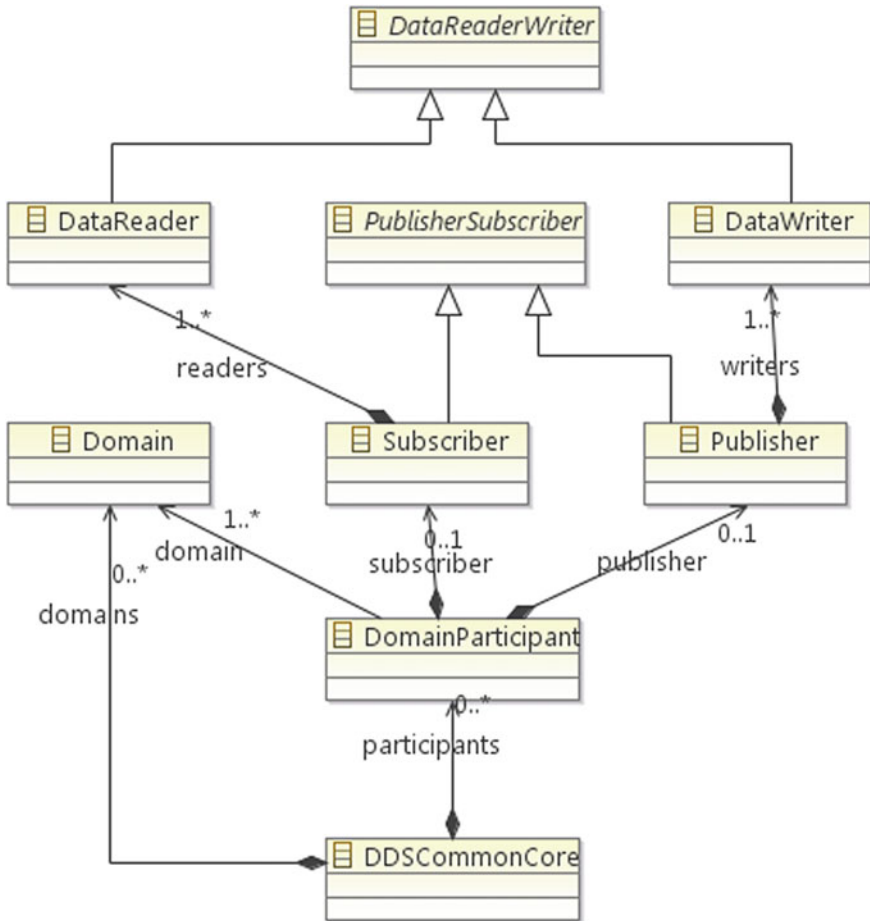


Fig. 5.7 Metamodel for DDS UML profile/DCPS/DCPS package

Typically, the architecture design phase follows the requirements analysis process. We assume that the requirements analysis phase is performed using the approaches as defined in the literature (e.g., rational unified process [5]) and provides the input for the DDS-based system architecture. The architecture of the DDS application is designed using the DDS UML profile. This includes the definition of the DDS types, the DDS topics, the domain participants, and the publish–subscribe relations.

Figures 5.14 and 5.15 show sample design diagrams for the traffic case study that uses the developed DDS UML profile. Figure 5.14 shows the definition of DDS types. For example, an incident has three fields which are incident ID, incident latitude, and incident longitude.

Figure 5.15 shows high-level design of the case study. Vehicles, sensors, and the managers are the domain participants. The publish–subscribe topics all join to the

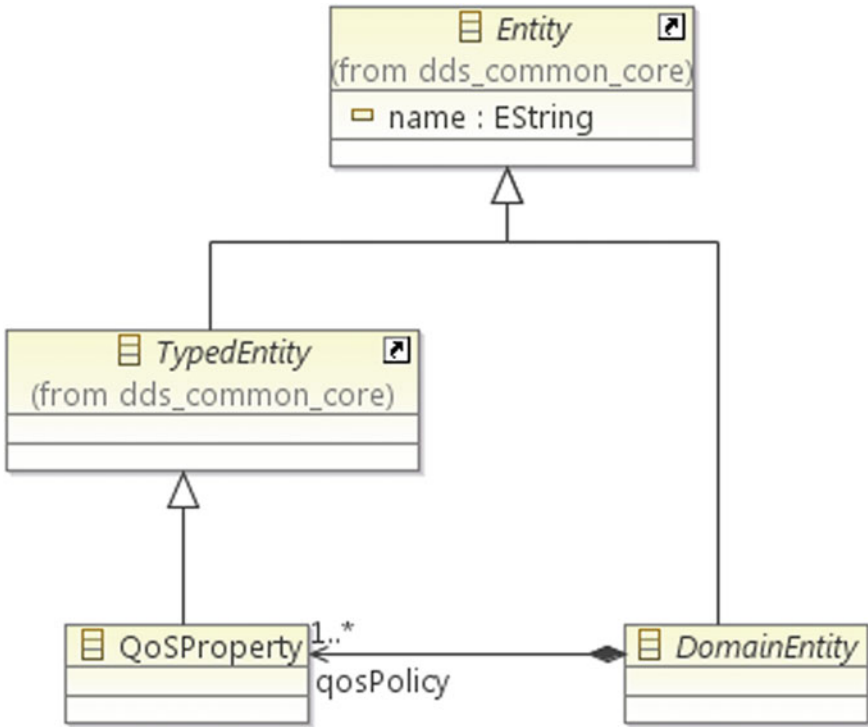


Fig. 5.8 Metamodel for DDS UML profile/DCPS/domain package

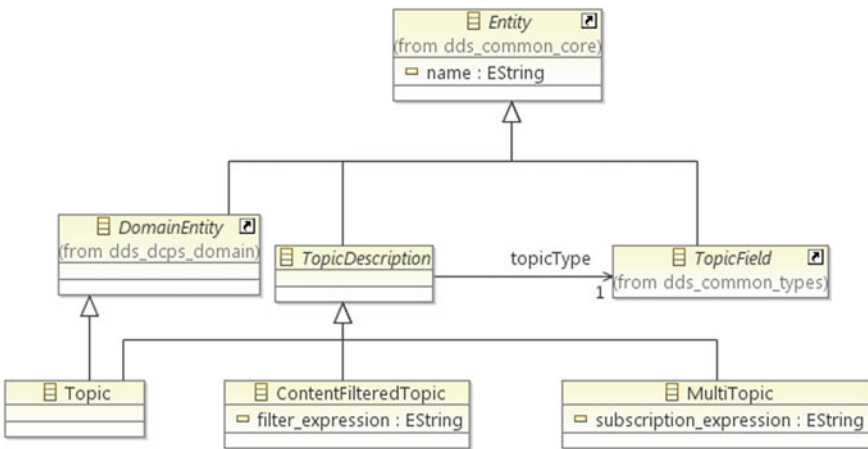


Fig. 5.9 Metamodel for DDS UML profile/common/topic package

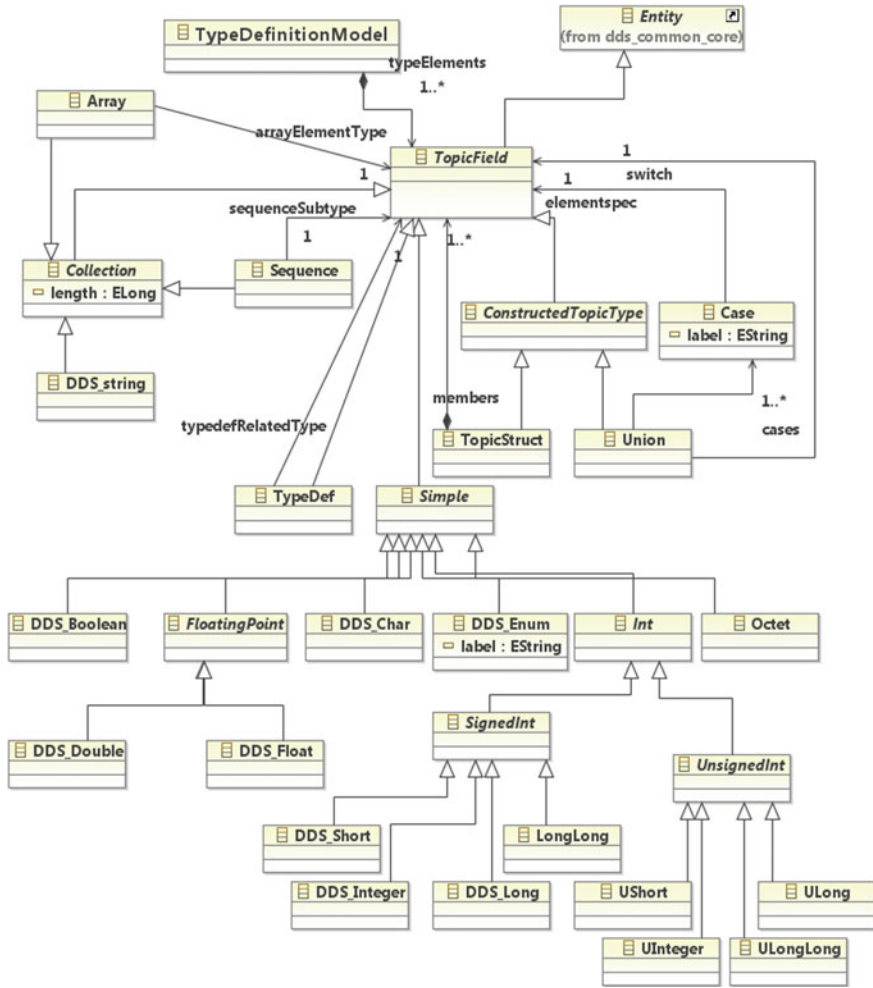


Fig. 5.10 Metamodel for DDS UML profile/common/types package

same domain. Note that, in Fig. 5.15, the fonts are not meant to be readable. The tool itself provides the functions to zoom in and out to analyze the specific elements.

### 5.7 Related Works

The work in this chapter is related to and enhances our earlier work. In [4], we have provided a systematic literature review to describe the state of the art of the DDS middleware and identified the obstacles in applying DDS. From this secondary

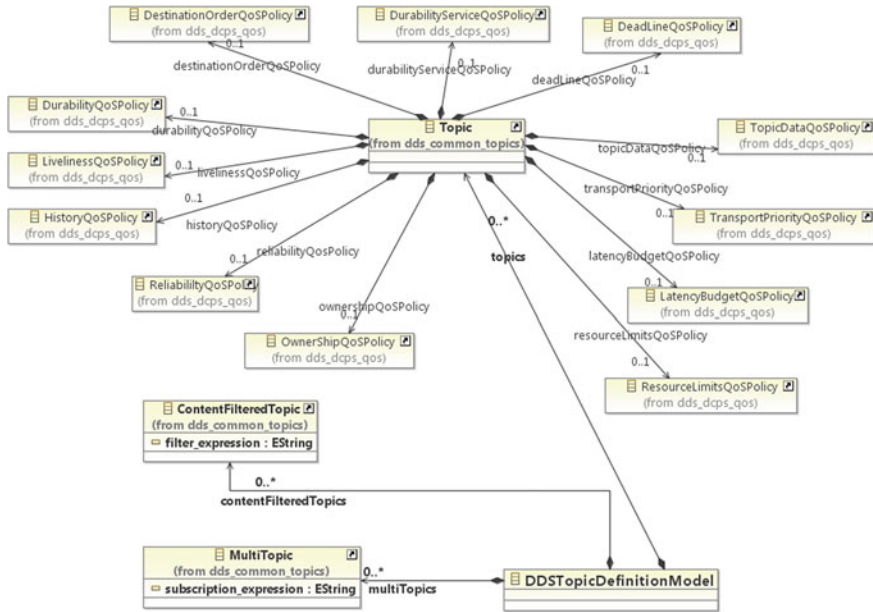


Fig. 5.11 Topic definition metamodel

study, we observed that the application of DDS has been increasingly popular, and it has been used in various application domains such as defense, finance, and medical domain. In addition to its basic application, we can also identify the application and integration of DDS to solve problems in technical domains such as cloud computing, component-oriented development, mobile computing, and wide area network. Our study further showed that DDS provides some important benefits for realizing real-time distributed applications. Using the SLR, we also identified 11 basic categories of problems that were discussed in the identified primary studies. The identified problems included complexity of DDS configuration, performance prediction, measurement and optimization, implementing DDS, DDS integration over WAN, DDS using wireless networks and mobile computing, interoperability among DDS vendor implementations, data consistency in DDS, reliability in DDS, scalability in DDS, security, and integration with event-based systems. In this chapter, we have focused on its application to IIoT and in particular the need for an explicit UML profile to support the modeling. Hence, this study is new and complementary to the earlier studies on DDS. Furthermore, we can state that most of the 11 problems that we identified largely apply to DDS-based Industrial IoT.

In [19], we have provided a systematic method for architecture design of DDS-based IoT systems. Here, we have adopted architecture viewpoints for modeling DDS, IoT, and finally, DDS-based IoT systems. Since both the DDS and IoT are often represented as layered structures, we have applied the layered viewpoint to represent the DDS-based IoT. Further, we have also defined the deployment view



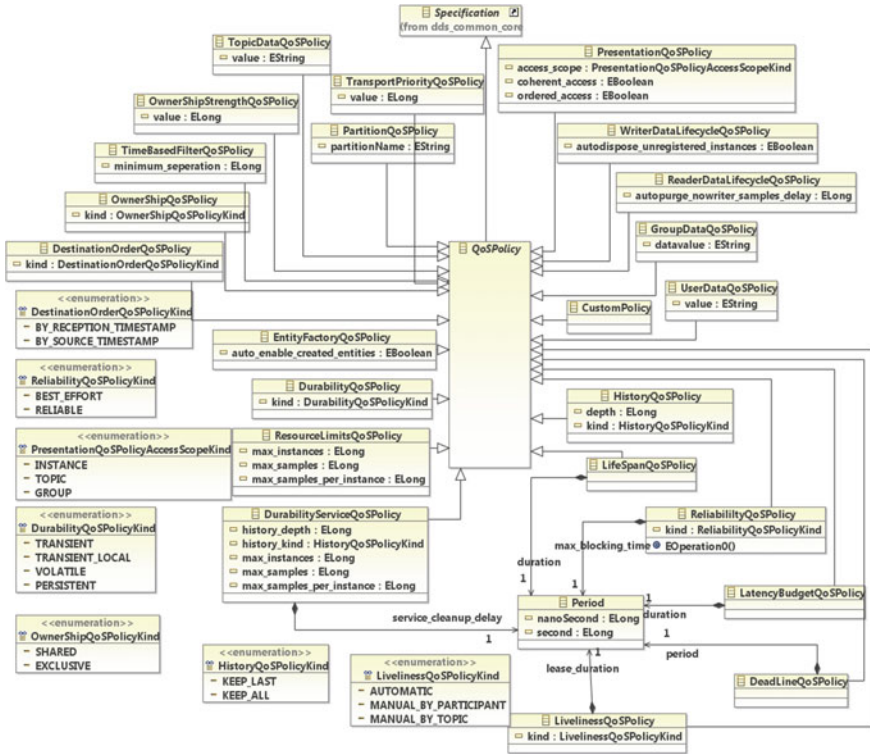
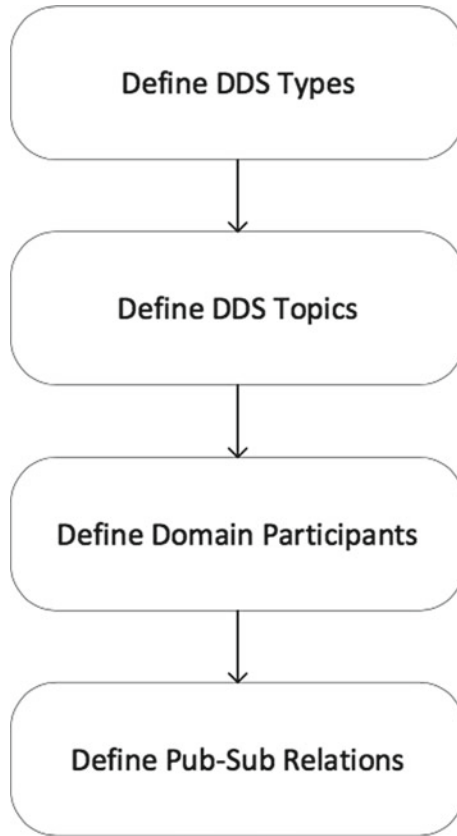


Fig. 5.12 Metamodel for DDS UML profile/DCPS/QoS package

for DDS-IoT and succeeded to integrate and represent the architecture models that can be used to model DDS-based IoT systems for various application domains. In this chapter, we did not focus on the design aspects, but considered the modeling of DDS-based IIoT systems. A pattern-based approach has been provided for designing IoT-based systems in [17]. In our future work, we will consider the design of DDS-based IIoT systems in more detail.

In [18], we address the problem of the selection of deployment alternatives given the application model, the physical resources, and the execution configurations, which is usually an intractable problem for the human engineer. Here, a systematic approach is provided that depicts the space of design alternatives and derives the most feasible deployment. This chapter elaborates on and enhances the earlier work but focuses on modeling. The adoption of the DDS UML profile will facilitate the design process.



**Fig. 5.13** Activity flow of DDS-based application design

## 5.8 Conclusion

IIoT-based systems are typically distributed systems characterized by their data-intensive and asynchronous behavior in which the quality of service parameters need to be carefully defined. To reduce the effort for developing distributed systems, common middleware architectures have been introduced. A middleware that is directly related to data-intensive systems in which quality of service parameters is explicitly considered is the Data Distribution Service (DDS) middleware. The DDS provides a standard data-centric publish–subscribe programming model and specification for distributed systems. In addition, the OMG has provided the DDS UML profile to support the modeling of the DDS applications.

We have provided an approach for extending the DDS UML profile for the context of IIoT. The approach has shown to be useful in the modeling and the design of DDS-based distributed applications. In particular, the direct focus on the data-intensive characteristics and the explicit means for modeling the QoS parameters appear very

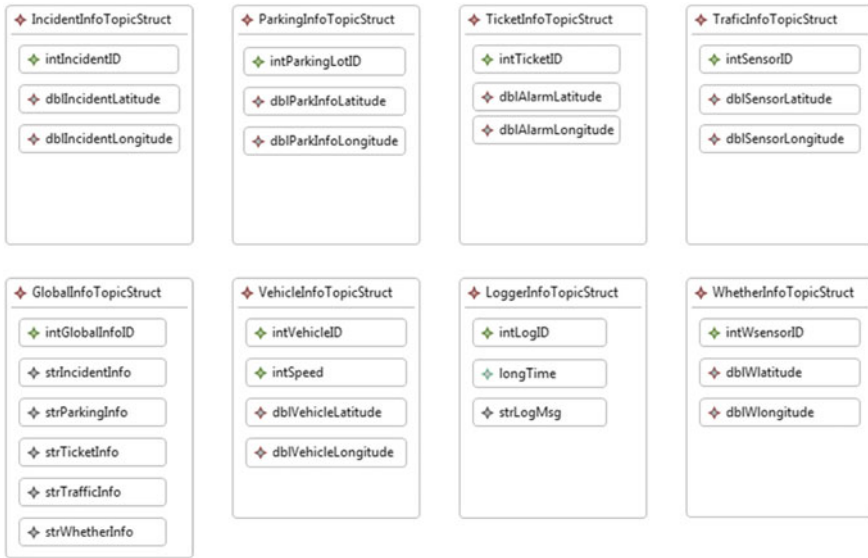


Fig. 5.14 Defining DDS types

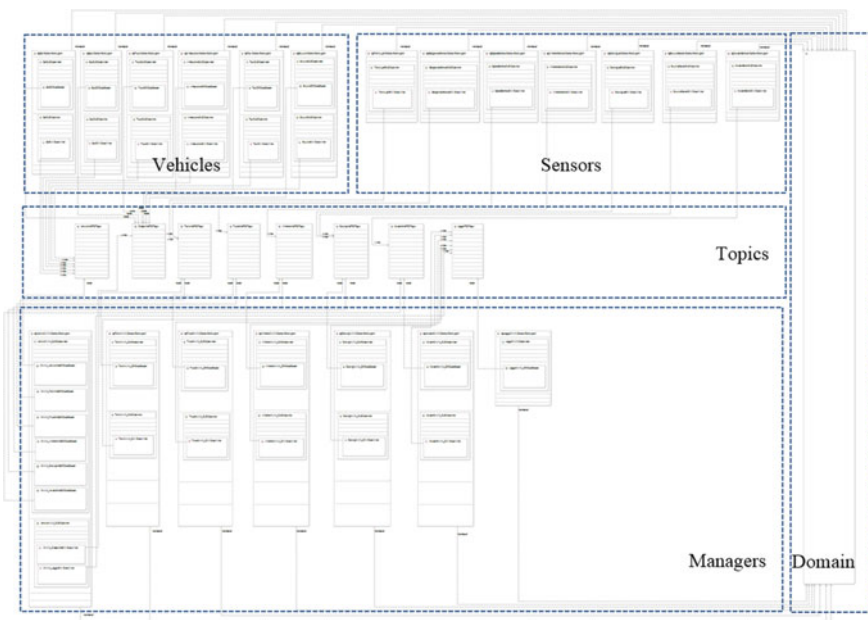


Fig. 5.15 High-level view of the DDS application design for the case study

useful for designing IIoT systems. In our future work, we will discuss further research work on extension and specialization of the suggested approach and elaborate on the specific quality factors in the context of IIoT. Furthermore, we will focus on the application of the profile in the overall IIoT design process.

## References

1. Eugster P, Felber PA, Guerraoui R, Kermarrec A (2003) The many faces of publish/subscribe. *J ACM Comput Surv* 35(2):114–131
2. IEEE 1998 (1998) IEEE STD 1278.1A-1998: standard for distributed interactive simulation—application protocols
3. IEEE 2010 (2010) IEEE STD 1516-2010 standard for modeling and simulation (M&S) high level architecture (HLA)—framework and rules
4. Köksal Ö, Tekinerdogan B (2017) Obstacles in data distribution service middleware: a systematic review. *Future Gener Comput Syst* 68:191–210. <https://doi.org/10.1016/j.future.2016.09.020>
5. Kruchten P (2003) The rational unified process: an introduction. *Science*. <https://doi.org/10.1109/ICSE.2002.146346>
6. Myerson J (2002) *The complete book of middleware*, Routledge
7. OMG (2018) OMG. Retrieved 17 May 2018 from <http://www.omg.org>
8. OMG (2010) DDS UML Profile—beta1. Retrieved from <http://www.omg.org/cgi-bin/doc?ptc/10-05-17.pdf>
9. OMG (2015) DDS + DLRL specification V 1.4. Retrieved from <https://www.omg.org/spec/DDS-DLRL/About-DDS-DLRL/>
10. OMG (2015) DDS specification V 1.4, 180. Retrieved from <http://www.omg.org/spec/DDS/1.4/>
11. OMG (2007) *Data distribution service for real-time systems*, Ver 1.2
12. Oracle (2002) *Java message service specification*, Ver 1.1
13. Pardo-castellote G, Farabaugh B, and Warren R (2005) *An introduction to DDS and data-centric communications*. Real-Time Innovations
14. Sparx Systems. (n.d.). *Enterprise architect UML modeling tool*. Retrieved 10 Mar 2018 from <http://sparxsystems.com/>
15. Steinberg D (2009) *EMF: eclipse modeling framework*. Addison-Wesley
16. Tekinerdogan B (2014) *Software architecture*. Computing handbook, 3rd edn. Chapman and Hall/CRC, pp 1–16
17. Tekinerdogan B and Köksal Ö (2018) Pattern based integration of Internet of Things systems. In: *International conference on Internet of Things*, Springer, pp 19–33
18. Tekinerdogan B, Celik T, Köksal Ö (2018) Generation of feasible deployment configuration alternatives for data distribution service based systems. *Comput Stand Interfaces* 58:126–145. <https://doi.org/10.1016/J.CSI.2018.01.002>
19. Tekinerdogan B, Celik T (2017) Architecting feasible deployment alternatives for publish-subscribe systems. *Int J Comput Softw Eng* 2:117 <https://doi.org/10.15344/2456-4451/2017/117>
20. Tekinerdogan B, Celik T, and Köksal Ö (2017) Data distribution service-based architecture design for the Internet of Things systems. In: Mahmood Z (ed) *Connected environments for the Internet of Things*, Springer, pp 269–285

# Chapter 6

## Industrial IoT Projects Based on Automation Pyramid: Constraints and Minimum Requirements



**J. A. López-Leyva, A. Talamantes-Álvarez, M. A. Ponce-Camacho, O. Meza-Arballo, B. Valadez-Rivera and L. Casemiro-Oliveira**

**Abstract** The industrial sector requires to improve the quality of processes to increase competitiveness. In addition, interconnectivity has seen a huge development based on teamwork related to hardware and software, which is the basis of Industrial Internet of Things (IIoT) vision. In this context, the automation pyramid concept defines the integration of relevant technologies, based on several hierarchical levels of automation, that working correctly together can improve the quality of processes without high-end hardware and software requirements. Therefore, it is important to clarify the relationship between all levels of automation in the IIoT context, emphasizing that the backbone of the IIoT is the optimal design and implementation of hardware and software based on real constraints for particular users; in order to increase the level of effectiveness and competitiveness. This chapter presents the real constraints for IIoT projects related to the state of the art of each level of automation of the automation pyramid. It also proposes the general minimum requirements necessary to develop an optimum IIoT system. These minimum requirements will promote the use of optional hardware and software to relax the design and implementation of IIoT projects based on cost-effectiveness analysis. Finally, the minimum requirements proposed and the detail description of the log-

---

J. A. López-Leyva (✉) · A. Talamantes-Álvarez · M. A. Ponce-Camacho · O. Meza-Arballo · B. Valadez-Rivera

Center for Innovation and Design (CEID), CETYS University, Ensenada, Mexico  
e-mail: [josue.lopez@cetys.mx](mailto:josue.lopez@cetys.mx)

A. Talamantes-Álvarez  
e-mail: [ariana.talamantes@cetys.edu.mx](mailto:ariana.talamantes@cetys.edu.mx)

M. A. Ponce-Camacho  
e-mail: [miguel.ponce@cetys.mx](mailto:miguel.ponce@cetys.mx)

O. Meza-Arballo  
e-mail: [oscar.meza@cetys.mx](mailto:oscar.meza@cetys.mx)

B. Valadez-Rivera  
e-mail: [bernardo.valadez@cetys.mx](mailto:bernardo.valadez@cetys.mx)

L. Casemiro-Oliveira  
Universidade Federal Rural Do Semi-Árido—UFERSA, Mossoró, Brazil  
e-mail: [leiva.casemiro@ufersa.edu.br](mailto:leiva.casemiro@ufersa.edu.br)

ical topology for IIoT projects can be used as a roadmap to increase the industrial competitiveness based on efficient use of resources.

**Keywords** IoT · IIoT · Automation pyramid · Constraints · Cost-effectiveness · Competitiveness · Logical topology · Monitoring flow · Control flow · Optimal design · Minimum requirements

## 6.1 Introduction

Nowadays, interdisciplinary projects have been of much interest in several sectors of the society. For example, cybernetics is an important field which supports the research and innovation of health sciences, the mechatronic systems support a number of industrial sectors, renewable energy technical proposals support many activities, and all of these projects require efficiency management. In particular, the Internet of Things (IoT) is a current interdisciplinary field where everyday objects (e.g., lamps, refrigerators, smartphones, computers, among others) are connected via the Internet either through open or closed channels (e.g., wireless connection or copper cables, respectively) in order to share relevant real-time information between them or to send information to a central unit—all this without direct human intervention [1, 2]. Thus, a huge amount of information is shared and concentrated to monitor particular parameters to facilitate the analysis and decision making based on the desired performance, and also, to create important opportunities for people [3, 4].

Considering the aforementioned, the industrial sector related to products and services has adopted the IoT discipline to improve their own processes or resolve particular issues, which leads to resource and time savings. Thus, IoT applied in the industrial sector permits to improve the quality control, supply chain traceability, general supply chain efficiency, manufacturing processes, management systems, among other important advantages. Therefore, when the IoT concept is applied to industries, it is called Industrial Internet of Things (IIoT), also known as Industry 4.0 or I4.0. In fact, IoT and IIoT concepts share features such as permanent availability and intelligent devices connected in similar architectures and automation logic, which use particular standards for industrial, domestic, personal, and metropolitan applications. However, an IIoT system intends to support the industry competitiveness while the IoT system intends to increase the comfort level of people (although the personal competitiveness may be related to the personal comfort level) [5–7]. Also, any automation system proposal, including IoT and IIoT, can be represented using the automation pyramid concept, which establishes five hierarchical levels (field, control, supervisory, planning, and management) that describe how the technology is being integrated into several applications, mainly for industrial applications [8].

The general purpose of the automation pyramid is to create a well-defined automation system according to the particular activities and performance required. However, the theory described by the automation pyramid is very general, i.e., it is common to find high-end hardware and software at different automation levels. In particular, the

main problem is not the automation pyramid description, but the partial technical and management interpretations of particular users, which are, generally, industries with high acquisitive power. These industries carry out a rough analysis of the hardware and software needed for particular processes and services to increase their competitiveness, which means that systems with more or fewer capabilities than necessary will be acquired. In this case, the problem is hypothetical because the high acquisitive power permits a slight lack of technical and management information so that the negative effects can be minimized by the general profit. However, the scenario presented can be an important problem for industries with low or reduced acquisitive power. Sometimes, these industries analyze, in depth, the projects that involve hardware and software to improve the competitiveness using the minimum technical and management requirements. Clearly, the above mentioned does not generalize all the industries around the world, but in our opinion, it is an adequate approximation.

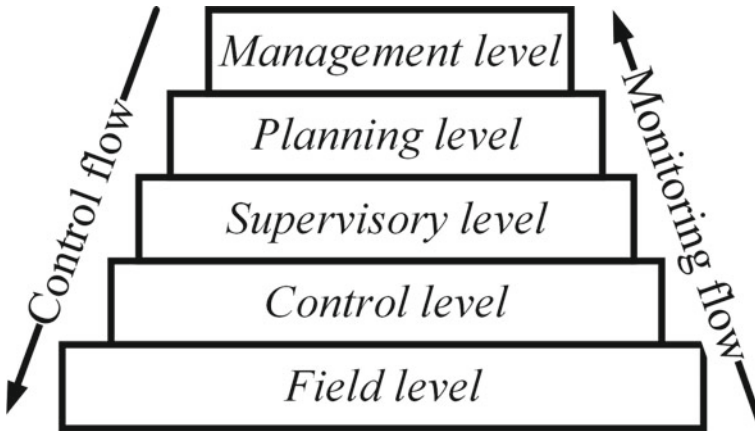
This chapter explains the real constraints that should be considered when designing and implementing an IIoT system in order to establish the minimum hardware and software requirements for each industry, which means important support to adequate the process to increase the competitiveness of users in particular conditions.

The chapter is organized as follows. Section 6.2 describes in detail the automation pyramid and the state of the art of the hardware and software used at each automation level to determine the particular real constraints in the IIoT context. Section 6.3 describes the minimum technical and management requirements to improve competitiveness. Finally, Sect. 6.4 presents the conclusion.

## 6.2 Automation Pyramid: Description, State of the Art and Constraints

To achieve the chapter's objective, it is important to define each level of the automation pyramid (see Fig. 6.1) to establish the requirements needed for IIoT applications.

- The first level (*Field level*) involves the basic instrumentation required for the physical work necessary for the automation process, for example, sensors, actuators, and other devices. In this case, these instrumentations are in direct contact with the process and, in general, can be defined as “dummy” (i.e., not smart) infrastructure.
- The second level (*Control level*) is considered the first smart level of the automation pyramid since it requires the information generated by the *Field level* infrastructure in order to make smart decisions. At this level, many control electronic devices can be used according to particular technical requirements and work area characteristics. For example, programmable logic controller (PLC), remote terminal unit (RTU), among other devices with the corresponding monitoring.
- The third level (*Supervisory level*) describes all the activities related to data acquisition from remote locations to perform high-level supervision and control from a unique location. These automation levels mentioned are commonly classified as *Operational Technology*.



**Fig. 6.1** Automation pyramid levels

- From the fourth level, we begin using the *Information Technologies*. Thus, the fourth level (*Planning level*) uses systems to monitor the complete processes of industry from the initial step (i.e., raw material supply) up to the end step (i.e., final product). In this case, articulated planning, that relates to manufacturing and management processes, is required. The manufacturing processes report to the *Planning level* the actual situation based on the interaction between the first three levels. It is important to clarify that the *Planning level* uses the information of all the production lines involved in an industry. This information is needed to make smart decisions related to required material, shipment plans, maintenance schedule, among others.
- Finally, the fifth level (*Management or Enterprise level*) is the highest automation level that integrates the monitoring and controlling of all the activities of the industry, such as all manufacturing processes, sales, purchases, and human resource details. Currently, some modifications or reductions to the automation pyramid have been proposed based on the fact that some particular tasks can be performed at various levels. However, the essence of the industrial automation model proposal remains constant.

In the following sections, we discuss, in some detail, the five levels of the automation pyramid.

### 6.2.1 *Field Level*

In this section, the basic task for the *Field level* instrumentation is presented, and based on that real constraints are shown. In addition, the state of the art is shown and analyzed considering the basic tasks and constraints. Thus, all the instrumentation used in the first automation level must be sensitive to all signals needed for a particu-



lar industrial process, such as indoor/outdoor weather conditions at the industry. This sensitivity means that the sensors produce an observable signal (mainly, electrical signal). In this point, the real industrial needs of each user have to be considered to determine the optimum instrumentation choice. Regarding the actuators, the technical capacity of each one is the principal constraint. Since the actuators and sensors are designed using different physical and technological backgrounds (i.e., electric, pneumatic, hydraulic, electromagnetic, mechanical, chemical, among others), it is important to evaluate the capabilities and interoperability between them. Therefore, the real constraints are highly related to the parameters and technical features according to the quality level desired by the industry. Thus, the first real constraint for IIoT at the lowest automation level is to clearly determine the quality desired for the process and services in order to choose the optimum sensors, actuators, and manufacturing machines. Clearly, this quality level is established from the highest automation levels and the *Field level* only focuses on contributing to guarantee the quality. In general, the minimization of errors and waste is desired to maintain or increase the quality and competitiveness, which means to clearly define the real constraints related to the parameters for the first automation level. Thus, the real constraints related to the quality and competitiveness are presented and defined as follows:

1. **Response time:** it describes the speed of the sensors, actuators, and manufacturing machines to do corresponding tasks. The principal trade-off regarding this statement is that the dynamic business process imposes the response time permitted so as not to delay shipments based on a particular order time and avoid overfilling the inventory.
2. **Precision:** it is related to accuracy. It describes the closeness between measurements. Thus, the entire infrastructure has to maintain adequate precision to optimize production efficiency, reduce the use of resources, and increase quality [9].
3. **Accuracy:** it describes the closeness of the sensor measurements, the action of the actuator, and the manufacturing activities that have to maintain a standard value close to the desired and designed value. Without ensured accuracy, it is difficult to ensure the quality of products or services.
4. **Intraoperatively:** it is related to compatibility between devices and brands in order to work together. In particular, compatibility means that different hardware and software can broadly share information and connection techniques to make an IIoT project more robust.
5. **Extra resources:** this considers the internal and external technical and operational support, maintenance, spare parts according to the lifetime of the element, equipment or machine, etc.
6. **Energy efficiency:** it is related to the use of minimum energy to perform an activity with the required quality of service. As support to industrial sustainability, this constraint is primordial since it procures an equilibrium related to the conventional sustainability concept and, in addition, among the other constraints.

All the real constraints mentioned are inputs to a cost-benefit analysis to determine the optimal resources that will be needed or used in the IIoT system. Based on the

**Table 6.1** State of the art of field level

Real constraints	Scientific and technical contribution
Response time	Time-sensitive networking [20], advanced algorithms [21], novel designs [22], wireless actuators [23]
Precision	Novel clock synchronization architecture [24], multilayer architectures [25], high-precision prediction modeling for sensors [26]
Accuracy	Advanced localization algorithms [27], distributed collaborative control [25], sampling and filtering to increase the accuracy of heterogeneous data [28]
Interoperatively	Reconfigurable smart sensor [29], optimizing mobile sensor and coverage [30, 31], novel middleware for connecting multiple devices [32]
Extra resources	Cross-layer infrastructure and cloud service [33], adaptive components for extra capabilities [34]
Energy efficiency	Novel codesign [35], cooperative industrial sensor [36], dense low-power sensor network [37], data centers use [38], optimized energy efficiency based on time-switching receiver design considering the maximum transmit power and the minimum harvested energy per user [39]

real constraints mentioned, a vast amount of technology exists which intends to cover the constraints. Next, a state of the art is presented to improve the performance or solve particular problems (see Table 6.1). However, a cost-benefit analysis is always needed because, perhaps, some state-of-the-art technologies are not required. If a nonintelligent and nonoptimal decision is made at the *Field level* considering the real constraints mentioned, all the higher levels of IIoT systems based on the automation pyramid will be affected, and so, quality and competitiveness will be decreased.

## 6.2.2 Control Level

All the input and output signals used at the *Field level* are received and transmitted by control units implemented at this level. These signals are used to make smart decisions about the production process at the lowest level within the industry. In general, some constraints mentioned for the *Field level* can be considered at the *Control level*, however some principal trade-offs and issues can be present in the devices and systems used at this level that impose particular constraints. In particular, PLC, RTU, distributed control systems (DCS), among other technical options, are suitable, although it is very difficult to distinguish the optimal uses with respect to each one. Therefore, the real constraints for IIoT systems at the *Control level* are highly related to the real constraints of the devices used at this level and the competitiveness parameters of each industrial user. Next, some constraints are listed:

1. **Analog or discrete process:** it considers the real actions performed by the industrial process. An analog process requires high-speed processing, which means generally high costs, while in a discrete process, a lower processing speed can be

tolerated. Although both analog and discrete signals are simultaneously embedded in industrial processes by high-speed analog-digital converters.

2. **Control techniques:** it is based on classical or modern control theories. Each production process requires particular control capabilities, controller, compensator, controller tuning, among other important actions to improve its performance. Thus, an analysis is required for each particular production process before selecting the control unit that satisfies the performance of the control parameters.
3. **Production information:** it describes not only the required control action but also the technical production information regarding all controlled devices for an individual or collective processes working together. This information can be reported and used as a first fire wall to detect and avoid future problems related to productivity. In this case, access to information at a remote location based on an Internet connection is highly desired.
4. **Scalability:** it refers to the amount of input and output signals that a device can handle and process. In the same context, it is related to the capability to handle other devices at the same automation level and at the lower level.
5. **Processing architecture:** it is related to the processing units used individually or jointly to increase the performance of the processes. For example, processors and field-programmable gate arrays (FPGA).
6. **Power consumption:** it describes the power consumed by a control unit in order to perform particular processing. Specifically, there is a direct relation between the complexity processing speed for the control algorithms and the power consumption parameter.
7. **Security for enterprise domain:** it refers to the security options to protect the information generated based on the production process. This information can be used by higher automation levels and so, affect the complete business operation.

According to the speed of the industrial processes, some devices are suitable for real-time applications. However, the response time of the second level is highly related to the response time of the first-level devices, and more importantly, to the required production time. In this respect, an important aspect is the lifetime of the devices used at the *Field* and *Control* levels. For the second level, devices with a long lifetime of 5–10 years are usually considered, while lifetime at the first level is relatively short. This condition imposes an important financial analysis when the IIoT systems are designed. Table 6.2 shows the state of the art related to each constraint mentioned.

### 6.2.3 Supervisory Level

In general, according to the analysis performed by a particular automation level, considering the higher levels, more information related to the overall industrial process is generated, and at the same time, more control information is required for the lower levels. Thus, at this level, the unified information regarding all the process of lower

**Table 6.2** State of the art of control level

Real constraints	Scientific and technical contribution
Analog or discrete process	High-resolution industrial monitor [40], improved electronic circuits, and transmission lines for high-speed I/O [41]
Control techniques	Nominal deterministic finite-state automaton-based model of the PLC control process [42], multicontrol distributed levels [43], optimal distributed elements control [44], output feedback fault-tolerant control and predictive compensation strategies [45]
Production information	Nontime-sensitive and time-sensitive data handled by fog computing and cloud computing [46], data logger and data archiving cloud storage for centralized data processing [47]
Scalability	scalable hardware/software architecture for multi/many-core PLCs [48], shared connecting areas (data aggregation and service cooperation) to connect divergent devices [49]
Processing architecture	Parallel programmable controller based on FPGAs [50], multi/many-core PLCs to reduce the scan cycle time [51], wide variety of processors such as Arduino Uno, Arduino Yun, Intel Galileo Gen 2, Intel Edison, Beagle Bone Black, Electric Imp 003, Raspberry Pi B+ and ARM mbed NXP LPC1768 [15]
Power consumption	low-swing global interconnection [52], power management for individual devices based on a powered center device [53], optimized communication protocols [54]
Security for enterprise domain	Mechanism to detect, analyze and remedy attacks [55], open source PLC modified to encrypt all data [56], calculating the uncertainty characterization of the PLC system [57], shifted time redundancy for error detection and correction [58]

levels (first and second levels) is needed in order to perform overall supervision and control in accordance with the productivity and the general performance parameters related to competitiveness. For these tasks, a supervisory control and data acquisition (SCADA) system is commonly used. In fact, the responsibility of the *Supervisory level* is to cover the communication between the *production* and the *management* levels (from the third to fifth level). For example, manufacturing operation management (MOM) system and manufacturing execution systems (MES) permit to control the production process performed at lower levels. These systems (MOM and MES) are described in the next section. Thus, the *Supervisory level* has important requirements that impose real constraints in order to communicate and control the lower automation levels and receive information from higher automation levels. Among the more important constraints, we have the following:

1. **Resilience level:** as aforementioned, *Supervisory level* is the medium level, so permanent use is required. Therefore, resilience level constraints mean that the downtime has to be minimized (or ideally, avoided).
2. **Connectivity performance:** the bandwidth and latency parameters are important to establish adequate communication between the devices and the systems of the lower levels with the other systems of the higher levels. Reduced bandwidth and

high latency can produce business decisions in nonreal time that affect productivity and competitiveness. In addition, availability is the primary requirement for connectivity performance, so local/remote access and monitoring are needed since the supervisory actions cannot be interrupted.

3. **Real-time processing:** it describes the processing speed related to the information rate in transmission and reception. It is important to clarify that real-time processing is somewhat subjective, i.e., the real concept should impose parallel processing. However, the real-time processing parameter is established considering the speed of the business model that involves all the automation levels.
4. **Secure access and confidentiality:** these define the access rules according to the risk level for a particular or overall industrial process. In fact, not all supervision processes need these features. In particular, unidentified interfaces, fire wall management, unknown services provided by third-party software, logical and physical configuration mismatch, and extended access to SCADA systems are potential vulnerabilities.
5. **Well-defined thresholds and keys:** these are required for all lower automation processes because this automation level performs supervision and control activities based on the acquired data. In particular, the key concept describes the important aspects that can be related to the other constraints mentioned, for example, authentication for users and systems at different levels, mutual communication ensured, among others.

The state of the art for the real constraints discussed above is now shown in Table 6.3.

### 6.2.4 Planning Level

This level needs enough information about different topics related to the complete business system, i.e., production information and internal/external management information. This information is required to plan the production, manage and track the resources (material, people, tools, time), which are necessary to make specific or general schedules related to quality control and generation of reports used to make smart business decisions.

It is clear that, at this level, mathematical models based on a learning method using data management are highly required. In particular, the MES technique helps to optimize productivity based on strictly real-time tracking and monitoring of all resources. In fact, sometimes the MOM system is considered the intermediary between the *Supervisory* and the *Management* levels. Next, some real constraints are presented and described according to the relationship with the other automation levels. Table 6.4 presents the state of the art related to the *Planning level* constraints.

1. **Monitoring features:** these are related to the historical statistical analysis and real-time data to determine the clear performance of the industrial processes,

**Table 6.3** State of the art of supervisory level

Real constraints	Scientific and technical contribution
Resilience level	Wireless sensor and actuator networks embedded into conventional supervisory systems to improve the dynamism, redundancy, fault tolerance, and self-organization [59]
Connectivity performance	Harmonize the standards to improve interoperability [60], optimize performance based on load data analysis [61], classify the type of information to be transmitted through the network to handle the operations in order to optimize the throughput network [45]
Real-time processing	Hardware-in-the-loop techniques and software integration [62], tracking states estimator for fast-rate processes and slow-rate supervisory system [63]
Secure access and confidentiality	Modern intrusion-tolerant protocols integrated to conventional systems [64], monitoring of available Internet-connected devices to avoid cyber attacks [65], multilayer cyber-security based on multiple attributes analysis [66], secure authentication protocols [67, 68]
Well-defined thresholds and keys	Impact of SCADA data accuracy on real-time processes [69], accuracy improvement based on frequency analysis [70], advanced and robust machine learning for robust thresholds calculated based on statistics [71]

**Table 6.4** State of the art of planning level

Real constraints	Scientific and technical contribution
Monitoring features	Offline and online analysis using statistical process and complex event processing models [72], oriented to provide useful information to the users of the manufacturing service provider, manufacturing service consumer, manufacturing service operator, among others [73], novel techniques used in the virtual factory concept [74]
Information kinds	Centering much information to improve the sustainability in industrial operations scheduling [75, 76], a great amount of concentrated information digitized increases the need for optimization techniques so as not to create a bottleneck for competitiveness decisions [77]
Basis of decision	Simultaneous and deterministic execution of control algorithms based on open-knowledge-driven [78], data mining techniques to improve the speed and robustness of processes [79], predictive scheduling based on hybrid control architectures [80], algorithms that use information from public cloud, private interenterprise cloud and manufacturing cloud regarding inbound/outbound logistics and mainstream processes to make smart decisions [20]

quality of service and products, and overall optimization. Sometimes an offline analysis is sufficient since the data variability is not extremely fast.

2. **Information kinds:** these refer to very large volumes of different kinds of data regarding manufacturing and management processes. These data are centralized and analyzed and considered as input signals to the complete business system. Thus, all information must be correctly processed and presented in the user interface without considering the information kind.
3. **Basis of decision:** it is related to the model used to produce output signals based on particular input signals. It is important to keep the rules well defined and available for a process of continuous improvement. Thus, proactive monitoring permits to make smart decisions.

### 6.2.5 Management Level

At the top level of the automation pyramid is the *Management level*. Recall that the lower automation levels perform particular tasks and, in general, higher levels monitor and control the lower levels considering the particular real constraints and requirements. In the same essence, the *Management level* uses all the information regarding the lower levels, i.e., it has a full view of all operations within a company, although it also requires external information. This action allows efficiency to be promoted based on continuous improvement processes and thus, improve quality, which leads to an increase in competitiveness. To perform these activities, ERP (enterprise resource planning) is commonly used since it allows to increase the productivity based on the information available (databases) at the same platform in order to save time and reduce costs. In addition, ERP systems allow the use of business intelligence tools to determine the actual enterprise status. The most important constraints and state of the art (see Table 6.5) related to this level are the following:

1. **Response time:** it is related to the time required to make smart decisions at the top automation level. It is clear that the response time is not the same as for the lower levels. In this scenario, the response time at this level highly depends on the dynamic of the market. Also, the connectivity status is highly related to the response time. In particular, connectivity is related to the interconnection capacity of the applications, software, hardware, and platforms used at this level, not only for communication with lower levels but also to communicate with the external infrastructure.
2. **Infrastructure for integration:** this is based on software, hardware, and databases needed to monitor and control in an integrated manner at all lower automation levels. If many platforms are used based on an in-depth technical analysis, a low integrated level is highly possible and, therefore, the decision-making process can require a lot of time with high uncertainty.

**Table 6.5** State of the art of management level

Real constraints	Scientific and technical contribution
Response time	Optimal update policy for the industrial database [81], prediction of cloud capacities for unstable service demands based on some algorithms to reduce service delays [82]
Infrastructure for integration	Technical support for the expansion of applications in the cloud for processes inside and outside the industry [83], optimized cloud and enterprise application integration based on cloud service bus [84], customized design of software for enterprise based on particular features [85], transformation of workloads using public/private/hybrid clouds [86]
Security	Analysis of critical success factor related to compliance, network, and security based on strict modeling [87]
Data accuracy	Component-level asset granularity to obtain specific and timeliness information required [81, 88], enterprise cognitive computing industrial applications in order to make complex decisions based on an ambiguous business context [89]

3. **Security:** this is extremely important because all the lower levels (inside the company) depend on the decisions taken at this level. In addition, information from outside the company (e.g., finance, accounting, human resources, sales, purchasing, payroll, etc.) cannot be available for arbitrary personnel.
4. **Data accuracy:** it is referred to the fact that all the lower automation levels send different types of information (related to manufacturing, human resources, finance, processing time, among others) to higher levels. Finally, complete or partial information is stored and used by the top level according to the operational rules established. Thus, degradation of accuracy based on particular problems at different levels of automation is possible. Therefore, data accuracy is highly required to make smart decisions according to industry reality.

Finally, the IIoT constraints (relating to the five levels) as already mentioned can be related to the conventional management theory for organizations, where four stages (control, direction, organization, and planning) are commonly used, as Fig. 6.2 shows. In fact, the IIoT system explained using the automation pyramid is a cybernetic system approach for industrial business management, which means that some challenges presented in the context of conventional management are very similar to the IIoT systems. Clearly, there are also some relevant differences between them, mainly those related to hardware and software [10].



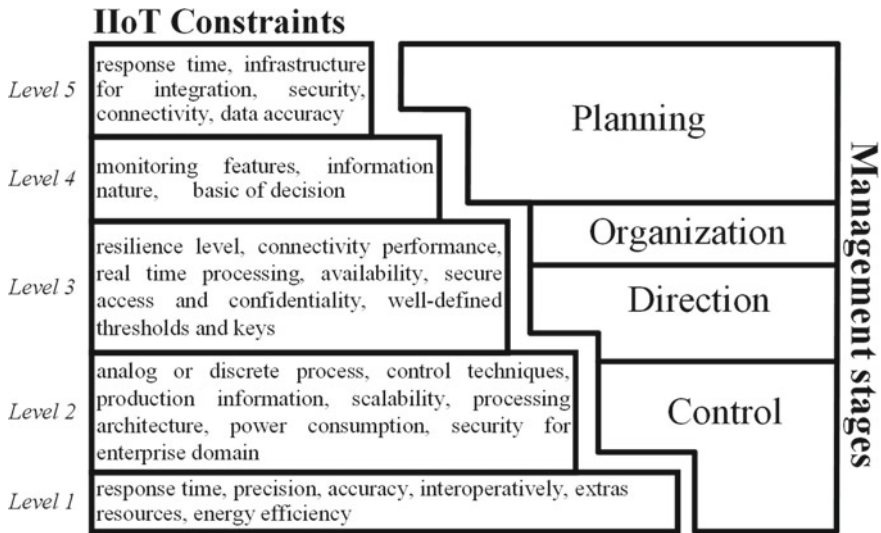


Fig. 6.2 Automation pyramid levels

### 6.3 Minimum Requirements for IIoT Projects

Currently, IIoT projects can be analyzed using the conventional automation pyramid. However, the cloud computing technique and high-end hardware and software are suitable options that work through the Internet and impose a conceptual modification of the physical topology automation pyramid to a logical topology automation pyramid. Thus, all actions performed by each automation level must still be performed, but now it is possible to use the Internet to generate a local/global link considering static/dynamic data and services provided by different systems (see Fig. 6.3).

In particular, monitoring and control flows are still used, only security cross-layers are added between conventional automation levels. Although there are some IIoT architecture proposals that involve multilayer related to data acquisition, business logic, identification, classification, communication, and control activities [10, 11]. However, the minimum requirements are not yet considered for these architectures.

Therefore, the minimum requirements are not completely related to the available high-end hardware and software because this means that the IIoT projects are not available for small and medium companies. In fact, the minimum requirements are associated with some particular industrial features to reach a particular competitiveness level using IIoT technology at the same time, which is related to specific costs, e.g., a cost-effectiveness analysis (CEA) for IIoT project is required to analyze the desired industrial competitiveness. In order to clarify, the complete minimum requirements are related to the overall performance regarding the hardware, software, cost, and effectiveness for a particular IIoT system to reach wanted competitiveness. Thus, the minimum requirements are proposed as follows:

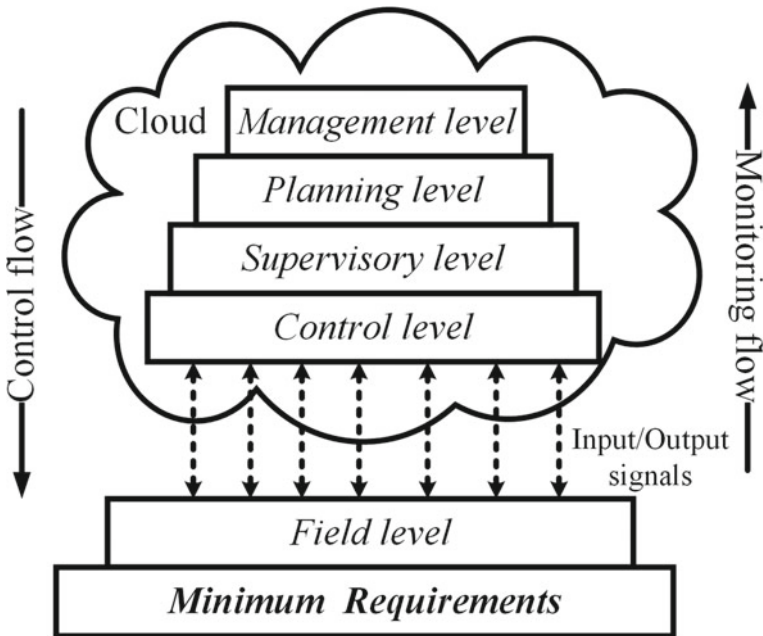


Fig. 6.3 Proposal logical topology for the automation pyramid

1. **Well-defined internal and external industrial processes:** these are important for the industry to clearly define the internal organizational structure. The clear definition involves all the internal processes related to all the automation levels. Also, for higher automation levels, external processes are required. If a company does not fully define the processes, the IIoT project will be an impossible task since the high-end hardware and software cannot fix the management mistakes related to the internal/external organization. In this context, the size and kind of the enterprise/company do not matter. In fact, there are small companies with well-defined processes while other large companies do not give such importance.
2. **Well-defined parameters for each hypothetical automation level:** in general, each internal/external process must have particular important parameters as input and output data to perform their particular tasks. Next, these parameters have to be classified and assigned to particular automation levels according to what was mentioned in the previous sections (i.e., characteristics and real constraints of automation levels).
3. **Well-defined intraoperatively features and communication processes between hypothetical automation levels:** an overall and well-defined process considers intraoperatively between all the stages of the process based on sharing features and a communication process to share information. Thus, control and monitoring information flows are defined. If a company has a well-defined particular process, but this process cannot communicate and understand with other processes, the IIoT project will have a major problem.

4. **Well-defined lean production based on a systematic method for waste minimization:** also called lean manufacturing, where the primary objective is to reduce all waste in the production processes related to internal and external industrial processes. In other words, it is not possible to make an overall IIoT project considering the automation of waste, i.e., firstly, waste minimization is a requirement. In order to do that, information, material, and personnel flows have to be ensured [12, 13].
5. **Competitiveness level desired:** another requirement before the implementation of an IIoT project is the competitiveness level desired to reach when the IIoT system is implemented. In fact, this requirement may be the most difficult to establish and measure by the company, since the parameters to measure the competitiveness level are established according to the mission and vision of the company. Usually, the industry does not consider this requirement based on a low uncertainty related to the IIoT marketing. However, it is important to clarify that not all IIoT projects implemented ensure an increase in the competitiveness level when the planning project does not consider these parameters.

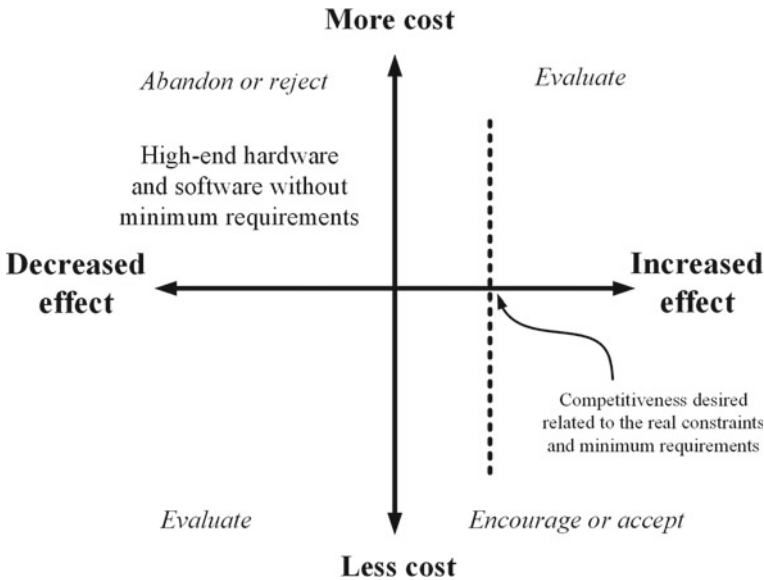
In general, the minimum requirements mentioned can be described using, e.g., the Toyota house philosophy [14]. Thus, the minimum requirements establishment is the first step in order to plan an IIoT project as shown in Fig. 6.3, where the basis of the novel automation pyramid is the aforementioned requirements. On the other hand, the minimum requirements and real constraints mentioned impose effectiveness related to the competitiveness level desired at the cost related to the wanted competitiveness. Therefore, any company that intends to begin an IIoT project have to consider the cost-effectiveness analysis (CEA).

Figure 6.4 shows a graphical cost-effectiveness analysis where the parameters mentioned are related (i.e., competitiveness and cost). Thus, there are four scenarios as follows:

- competitiveness increase requiring more cost
- competitiveness increase requiring less cost
- competitiveness decrease requiring more cost
- competitiveness decrease requiring less cost.

In particular, the ideal scenario is when an IIoT project considers all the minimum requirements and real constraints to increase the competitiveness with a lower cost, which is highly desirable. However, another scenario close to the ideal is to reach the desired competitiveness with a higher cost, which means that a depth evaluation is needed to reduce the cost. In order to clarify, sometimes IIoT projects have a strongly reduced probability of success because the proposed high-end hardware and software do not take into account the minimum requirements and real constraints, and thus increasing the cost and decreasing the IIoT effect, i.e., reducing the competitiveness. These IIoT projects are most likely to be abandoned or rejected.

Considering the aforementioned, an important minimum requirement is also the financial situation and investment budget that the company considered necessary to increase its competitiveness.



**Fig. 6.4** Cost-effectiveness analysis for IIoT projects considering minimum requirements

What has been previously mentioned imposes minimum requirements for the hardware and software used in IIoT projects in a logical topology for the automation pyramid. It also considers the real constraints related to each automation level. For example, the hardware and software classified as *Commercial Off-The-Shelf* (COTS) and low-cost programmable controllers are the available options for *Field* and *Control* levels. Commonly, these options use freely available easy-to-use programming software. However, these options must be analyzed using the real constraints, as mentioned in Sects. 6.2.1 and 6.2.2, according to the particular needs of the industrial processes and the required competitiveness level.

Depending on the competitiveness level desired, some parameters of specific devices should be analyzed in depth, such as clock speed, bus width, system memory, supported communication, development environments, programming language, and connectivity [15]. Regarding the three higher automation levels (*Supervisory*, *Planning*, and *Management*), there is a large amount of multipurpose software with outstanding flexibility and connectivity performance between others platforms [16–19]. Also, these options have to be analyzed using the real constraints as mentioned in Sects. 6.2.3 and 6.2.5.

In order to further explain, some tasks performed at the higher automation levels are defined based on internal and external industrial rules (e.g., warnings, thresholds, operational and manufacturing management, planning information about all the business industrial model, external information related to the customers, among others), so it is difficult to be specific about these tasks.

## 6.4 Conclusion

Nowadays, the roadmap for the implementation of an IIoT project is not clear at all. Although the IIoT paradigm is a highly attractive topic for research as well as for applications for the industry and academic sectors, it mainly refers to particular research lines, e.g., improvement of the technical performance, integration level, security, and management issues. Thus, the misconception that the IIoT directly increases the competitiveness of any industry without performing a complete analysis of the pertinence is the most important factor to reduce the probability of success of any IIoT project.

This chapter has presented the conventional automation pyramid and its relation with the IIoT projects. A summary of the state of the art and the real constraints related to conventional automation levels has also been provided. The aforementioned helps to determine the minimum requirements needed for any company in order to implement an IIoT system to increase the competitiveness level. In fact, increasing the competitiveness of any company is the main objective when an IIoT system is implemented for the supply chain.

It is evident that if the competitiveness is not increased based on a previous formal cost-effectiveness analysis, an IIoT system proposal is not suitable for a particular application. Hence, conventional management and industrial techniques/tools should be used first to improve competitiveness relating to the IIoT system planning.

Additionally, the minimum requirements needed to begin the analysis of a potential IIoT project are proposed and defined. Thus, well-defined internal and external industrial processes, clear parameters for each hypothetical automation level, detailed intraoperatively features and communication processes between hypothetical automation levels, implementation of lean production based on a systematic method for waste minimization, the establishment of competitiveness level desired, and the financial support are the minimum requirements defined.

In this context, the use of the business process management maturity (BPMM) model is highly recommended to determine the maturity of the organizational process. Consequently, the maturity level can support the decision of whether an IIoT project should or should not be started.

Our future work involves the investigation of a clear roadmap to implement IIoT systems in the industry (or any particular company) based on well-defined stages, real constraints, and minimum requirements to determine the probability of success regarding the competitiveness level desired.

## References

1. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. *Comput Netw* 54:2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
2. Whitmore A, Agarwal A, Xu LD (2015) The internet of things—a survey of topics and trends. *Inf Syst Front* 17:261–274. <https://doi.org/10.1007/s10796-014-9489-2>

3. Marr B (2015) Big data: using SMART big data, analytics and metrics to make better decisions and improve performance. Wiley, Chichester
4. Mazhar Rathore M, Ahmad A, Paul A, Rho S (2016) Urban planning and building smart cities based on the internet of things using big data analytics. *Comput Netw* 101:63–80. <https://doi.org/10.1016/j.comnet.2015.12.023>
5. Hatzivasilis G, Fysarakis K, Soultatos O, Askoxylakis I, Papaefstathiou I, Demetriou G (2018) The industrial internet of things as an enabler for a circular economy Hy-LP: a novel IIoT protocol, evaluated on a wind park's SDN/NFV-enabled 5G industrial network. *Comput Commun* 119:127–137. <https://doi.org/10.1016/j.comcom.2018.02.007>
6. Mumtaz S, Alsohaily A, Pang Z, Rayes A, Tsang KF, Rodriguez J (2017) Massive Inter-net of things for industrial applications: addressing wireless IIoT connectivity challenges and ecosystem fragmentation. *Ind Electr Mag* 11:28–33. <https://doi.org/10.1109/MIE.2016.2618724>
7. Popescu GH (2015) The economic value of the industrial internet of things. *J Self-Gov Manage Econ* 3:86–91
8. Jeschke S, Brecher C, Meisen T, Özdemir D, Eschert T (2017) Industrial internet of things and cyber manufacturing systems. In: Jeschke S, Brecher C, Song H, Rawat D (eds) *Industrial internet of things*. Springer series in wireless technology. Springer, Cham
9. Ferrández-Pastor FJ, García-Chamizo J, Nieto-Hidalgo M, Mora-Pascual J, Mora-Martínez J (2016) Developing ubiquitous sensor network platform using internet of things: application in precision agriculture. *Sensors* 16:1141–1161. <https://doi.org/10.3390/s16071141>
10. Du S, Liu B, Ma H, Wu G, Wu P (2018) IIOT-based intelligent control and management system for motorcycle endurance test. Access 6:30567–30576. <https://doi.org/10.1109/ACCESS.2018.2841185>
11. Tie Q, Wu DO, Prathap P (2017) Introduction to the special section on software architecture and modeling for industrial internet of things. *Comput Elect Eng* 58:241–243. <https://doi.org/10.1016/j.compeleceng.2017.04.022>
12. Bauer H, Brandl F, Lock C, Reinhart G (2018) Integration of industrie 4.0 in lean manufacturing learning factories. *Procedia Manuf* 23:147–152. <https://doi.org/10.1016/j.promfg.2018.04.008>
13. Sanders A, Elangeswaran C, Wulfsberg J (2016) Industry 4.0 implies lean manufacturing: research activities in industry 4.0 function as enablers for lean manufacturing. *J Ind Eng Manage* 9:811–833. <https://doi.org/10.3926/jiem.1940>
14. Krijnen A (2007) The toyota way: 14 management principles from the world's greatest manufacturer. *Action Learn Res Practice* 4:1109–1111. <https://doi.org/10.1080/14767330701234002>
15. Ray PP (2018) A survey on internet of things architectures. *J King Saud Univ Comput Inf Sci* 30:291–319. <https://doi.org/10.1016/j.jksuci.2016.10.0031>
16. Adamo F, Attivissimo F, Cavone G, Giaquinto N (2007) SCADA/HMI systems in advanced educational courses. *Trans Instrum Meas* 56:4–10. <https://doi.org/10.1109/TIM.2006.887216>
17. Biswal GR, Maheshwari RP, Dewal ML (2012) Modeling, control, and monitoring of S3RS-based hydrogen cooling system in thermal power plant. *Trans Ind Electr* 59:562–570. <https://doi.org/10.1109/TIE.2011.2134059>
18. Romero-Acero A, Marin-Cano A, Jimenez-Builes JA (2014) SCADA system for detection of explosive atmospheres in underground coal mines through wireless sensor network. *Latin Am Trans* 12:1398–1403. <https://doi.org/10.1109/TLA.2014.7014506>
19. Tyagi H, Yadav R, Patel K, Bandyopadhyay M, Rotti C, Sudhir D, Gahlaut A, Pandya K, Chakraborty A, Trivedi T (2017) Development of data acquisition and control system for long pulse operations of Indian test facility of ITER DNB. *Trans Nucl Sci* 64:1426–1430. <https://doi.org/10.1109/TNS.2017.2684243>
20. Wollschlaeger M, Sauter T, Jaspermeite J (2017) The future of industrial communication: automation networks in the era of the internet of things and industry 4.0. *Ind Electr Mag* 11:17–27. <https://doi.org/10.1109/MIE.2017.2649104>
21. Tahir Y, Yang S, McCann J (2018) BRPL: backpressure RPL for high-throughput and mobile IoTs. *Trans Mobile Comput* 17:29–43. <https://doi.org/10.1109/TMC.2017.2705680>

22. Lopes De Faria ML, Cugnasca CE, Amazonas JRA (2018) Insights into IoT data and an innovative DWT-based technique to denoise sensor signals. *Sens J* 18:237–247. <https://doi.org/10.1109/JSEN.2017.2767383>
23. Chen J, Cao X, Cheng P, Xiao Y, Sun Y (2010) Distributed collaborative control for industrial automation with wireless sensor and actuator networks. *Trans Ind Electr* 57:4219–4230. <https://doi.org/10.1109/TIE.2010.2043038>
24. Wang S, Hou Y, Gao F, Ma S (2016) A novel clock synchronization architecture for IoT access system. In: International conference on computer and communications, pp 1456–1459. <https://doi.org/10.1109/compcomm.2016.7924944>
25. Khattab A, Abdelgawad A, Yelmarthi K (2016) Design and implementation of a cloud-based IoT scheme for precision agriculture. In: International conference on microelectronics, 201–204. <https://doi.org/10.1109/icm.2016.7847850>
26. Zhang P, Liu Y, Wu F, Liu S, Tang B (2016) Low-overhead and high-precision prediction model for content-based sensor search in the internet of things. *IEEE Commun Lett* 20:720–723. <https://doi.org/10.1109/LCOMM.2016.2521735>
27. Yang P (2015) PRLS-INVES: a general experimental investigation strategy for high accuracy and precision in passive RFID location systems. *Internet Things J* 2:159–167. <https://doi.org/10.1109/JIOT.2014.2377351>
28. Sun Y, Song H, Jara AJ, Bie R (2016) Internet of things and big data analytics for smart and connected communities. *Access* 4:766–773. <https://doi.org/10.1109/ACCESS.2016.2529723>
29. Chi Q, Yan H, Zhang C, Pang Z, Xu LD (2014) A reconfigurable smart sensor interface for industrial WSN in IoT environment. *Trans Ind Inf* 10:1417–1425. <https://doi.org/10.1109/TII.2014.2306798>
30. Dou R, Nan G (2017) Optimizing sensor network coverage and regional connectivity in industrial IoT systems. *Syst J* 11:1351–1360. <https://doi.org/10.1109/JSYST.2015.2443045>
31. Qin Z, Wu D, Xiao Z, Fu B, Qin Z (2018) Modeling and analysis of data aggregation from convergecast in mobile sensor networks for industrial IoT. *Trans Ind Inf* 14:4457–4467. <https://doi.org/10.1109/TII.2018.2846687>
32. da Cruz MAA, Rodrigues JJPC, Al-Muhtadi J, Korotaev VV, de Albuquerque VHC (2018) A reference model for internet of things middleware. *Internet Things J* 5:871–883. <https://doi.org/10.1109/JIOT.2018.2796561>
33. Sheng Z, Mahapatra C, Zhu C, Leung VCM (2015) Recent advances in industrial wireless sensor networks toward efficient management in IoT. *Access* 3:622–637. <https://doi.org/10.1109/ACCESS.2015.2435000>
34. Oteafy SMA, Hassanein HS (2017) Resilient IoT architectures over dynamic sensor networks with adaptive components. *Int Things J* 4:474–483. <https://doi.org/10.1109/JIOT.2016.2621998>
35. Lyu L, Chen C, Zhu S, Guan X (2018) 5G enabled codesign of energy-efficient trans-mission and estimation for industrial IoT systems. *Trans Ind Inf* 14:2690–2704. <https://doi.org/10.1109/TII.2018.2799685>
36. Zhu R, Zhang X, Liu X, Shu W, Mao T, Jalaian B (2015) ERDT: energy-efficient reliable decision transmission for intelligent cooperative spectrum sensing in industrial IoT. *Access* 3:2366–2378. <https://doi.org/10.1109/ACCESS.2015.2501644>
37. Williams JM, Khanna R, Ruiz-Rosero JP, Pisharody G, Qian Y, Carlson CR, Liu H, Ramirez-Gonzalez G (2017) Weaving the wireless web: toward a low-power, dense wireless sensor network for the industrial IoT. *Microw Mag* 18:40–63. <https://doi.org/10.1109/MMM.2017.2740738>
38. Nwadiugwu WP, Kim D-S (2018) Energy-efficient sensors in data centers for industrial internet of things (IIoT). In: International conference on internet of things: smart innovation and usages, pp 1–6. <https://doi.org/10.13140/rg.2.2.31491.71208>
39. Tang J, So DKC, Zhao N, Shojaeifard A, Wong K (2018) Energy efficiency optimization with SWIPT in MIMO broadcast channels for internet of things. *Internet Things J* 5:2605–2619. <https://doi.org/10.1109/JIOT.2017.2785861>

40. Li Z, Xi J, He L, Sun K (2016) A front-end circuit with 16-channel 12-bit 100-kSps RC-hybrid SAR ADC for industrial monitoring application. In: Asia Pacific conference on circuits and systems, pp 340–343. <https://doi.org/10.1109/apccas.2016.7803970>
41. Zhang DC, Swaminathan M, Raychowdhury A, Keezer D (2017) Enhancing the bandwidth of low-dropout regulators using power transmission lines for high-speed I/Os. *Trans Compon Packag Manuf Technol* 7:533–543. <https://doi.org/10.1109/TCPMT.2017.2655002>
42. Ghosh A, Qin S, Lee J, Wang G (2017) FBMP: An automated fault and behavioral anomaly detection and isolation tool for PLC-Controlled manufacturing systems. *Trans Syst Man Cybern Syst* 47:3397–3417. <https://doi.org/10.1109/TSMC.2016.2633392>
43. Li Z, Zang C, Zeng P, Yu H, Li S (2018) Fully distributed hierarchical control of parallel grid-supporting inverters in islanded AC microgrids. *Trans Ind Inf* 14:679–690. <https://doi.org/10.1109/TII.2017.2749424>
44. Kohn W, Zabinsky ZB, Nerode A (2015) A micro-grid distributed intelligent control and management system. *Trans Smart Grid* 6:2964–2974. <https://doi.org/10.1109/TSG.2015.2455512>
45. Pramod TC, Boroojeni KG, Amini MH, Sunitha NR, Iyengar SS (2018) Key pre-distribution Scheme with join leave support for SCADA systems. *Int J Critical Infrastruct Prot* 2. <https://doi.org/10.1016/j.ijcip.2018.10.011>
46. Fu J, Liu Y, Chao H, Bhargava BK, Zhang Z (2018) Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. *Trans Ind Inf* 14:4519–4528. <https://doi.org/10.1109/TII.2018.2793350>
47. Kulkarni PH, Kute PD, More VN (2016) IoT based data processing for automated industrial meter reader using Raspberry Pi. In: International conference on internet of things and applications, pp 107–111. <https://doi.org/10.1109/iota.2016.7562704>
48. Canedo A, Ludwig H, Al Faruque MA (2014) High communication throughput and low scan cycle time with multi/many-core programmable logic controllers. *Embed Syst Lett* 6:21–24. <https://doi.org/10.1109/LES.2014.2299731>
49. Shen Y, Zhang T, Wang Y, Wang H, Jiang X (2017) MicroThings: a generic IoT architecture for flexible data aggregation and scalable service cooperation. *Commun Mag* 55:86–93. <https://doi.org/10.1109/MCOM.2017.1700104>
50. Hajduk Z, Trybus B, Sadolewski J (2015) Architecture of FPGA embedded multiprocessor programmable controller. *Trans Ind Electr* 62:2952–2961. <https://doi.org/10.1109/TIE.2014.2362888>
51. Wang T, Gao H, Qiu J (2016) A combined fault-tolerant and predictive control for network-based industrial processes. *Trans Ind Electr* 63:2529–2536. <https://doi.org/10.1109/TIE.2016.2515073>
52. Qi H, Ayorinde O, Calhoun BH (2017) An ultra-low-power FPGA for IoT applications. in: SOI-3D-Subthreshold Microelectronics Technology Unified Conference (S3S), pp 1–3. <https://doi.org/10.1109/s3s.2017.8308753>
53. Ikram W, Petersen S, Orten P, Thornhill NF (2014) Adaptive multi-channel transmission power control for industrial wireless instrumentation. *Trans Ind Inf* 10:978–990. <https://doi.org/10.1109/TII.2014.2310594>
54. Zhao M, Ho IW, Chong PHJ (2016) An energy-efficient region-based RPL routing protocol for low-power and lossy networks. *Internet Things J* 3:1319–1333. <https://doi.org/10.1109/JIOT.2016.2593438>
55. Ahmed I, Obermeier S, Sudhakaran S, Roussev V (2017) Programmable logic controller forensics. *Secur Priv* 15:18–24. <https://doi.org/10.1109/MSP.2017.4251102>
56. Alves T, Das R, Morris T (2018) Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. *Embed Syst Lett* 10:99–102. <https://doi.org/10.1109/LES.2018.2823906>
57. Zhang H, Jiang Y, Hung WNN, Song X, Gu M, Sun J (2014) Symbolic analysis of programmable logic controllers. *Trans Comput* 63:2563–2575. <https://doi.org/10.1109/TC.2013.124>
58. Cronin P, Hosseini FS, Yang C (2018) A low overhead solution to resilient assembly lines built from legacy controllers. *Embed Syst Lett* 10:103–106. <https://doi.org/10.1109/LES.2018.2829768>



59. Grilo AM, Chen J, Díaz M, Garrido D, Casaca A (2014) An integrated WSN and SCADA system for monitoring a critical infrastructure. *Trans Ind Inf* 10:1755–1764. <https://doi.org/10.1109/TII.2014.2322818>
60. Lee B, Kim D-K (2017) Harmonizing IEC 61850 and CIM for connectivity of substation automation. *Comput Stand Interfaces* 50:199–208. <https://doi.org/10.1016/j.csi.2016.10.008>
61. Enache D, Chenaru O, Popescu D (2016) Performance and load analysis for remote plant connectivity using GSM communication. In: *Telecommun Forum*, pp 1–4. <https://doi.org/10.1109/telfor.2016.7818744>
62. Montaña DAM, Rodriguez DFC, Ivan Clavijo Rey D, Ramos G (2018) Hardware and software integration as a realist SCADA environment to test protective relaying control. *Trans Ind Appl* 54:1208–1217. <https://doi.org/10.1109/TIA.2017.2780051>
63. Alcaide-Moreno BA, Fuerte-Esquivel CR, Glavic M, Van Cutsem T (2018) Electric power network state tracking from multirate measurements. *Trans Instrum Meas* 67:33–44. <https://doi.org/10.1109/TIM.2017.2754838>
64. Kirsch J, Goose S, Amir Y, Wei D, Skare P (2014) Survivable SCADA via intrusion-tolerant replication. *Trans Smart Grid* 5:60–70. <https://doi.org/10.1109/TSG.2013.2269541>
65. Samtani S, Yu S, Zhu H, Patton M, Matherly J, Chen H (2018) Identifying SCADA systems and their vulnerabilities on the internet of things: a text-mining approach. *Intell Syst* 33:63–73. <https://doi.org/10.1109/MIS.2018.111145022>
66. Yang Y, McLaughlin K, Sezer S, Littler T, Im EG, Pranggono B, Wang HF (2014) Multiattribute SCADA-specific intrusion detection system for power networks. *Trans Power Deliv* 29:1092–1102. <https://doi.org/10.1109/TPWRD.2014.2300099>
67. Amoah R, Camtepe S, Foo E (2016) Securing DNP3 broadcast communications in SCADA systems. *Trans Ind Inf* 12:1474–1485. <https://doi.org/10.1109/TII.2016.2587883>
68. Coffey K, Maglaras LA, Smith R, Janicke H, Ferrag MA, Derhab A, Mukherjee M, Rallis S, Yousaf A (2018) Vulnerability assessment of cyber security for SCADA systems. In: Parkinson S, Crampton A, Hill R (eds) *Guide to vulnerability analysis for computer networks and Systems. Computer communications and networks*. Springer, Cham
69. Choi D, Xie L (2014) Sensitivity analysis of real-time locational marginal price to SCADA sensor data corruption. *Trans Power Syst* 29:1110–1120. <https://doi.org/10.1109/TPWRS.2013.2293634>
70. Dong Q, Sun J, Wu Q, Liu Y (2017) A method for filtering low frequency disturbance in PMU data before coordinated usage in SCADA. *Trans Power Syst* 32:2810–2816. <https://doi.org/10.1109/TPWRS.2016.2615309>
71. Papatheou E, Dervilis N, Maguire AE, Antoniadou I, Worden K (2015) A performance monitoring approach for the novel Lillgrund offshore wind farm. *Trans Ind Electr* 62:6636–6644. <https://doi.org/10.1109/TIE.2015.2442212>
72. Almada-Lobo F (2015) The industry 4.0 revolution and the future of manufacturing execution systems (MES). *J Innov Manage* 3:16–21
73. Tao F, Cheng J, Cheng Y, Gu S, Zheng T, Yang H (2017) SDMSim: a manufacturing service supply-demand matching simulator under cloud environment. *Robot Comput Integ Manuf* 45:34–46. <https://doi.org/10.1016/j.rcim.2016.07.001>
74. Xu P, Mei H, Ren L, Chen W (2017) ViDX: visual diagnostics of assembly line performance in smart factories. *Trans Vis Comput Gr* 23:291–300. <https://doi.org/10.1109/TVCG.2016.2598664>
75. Giret A, Trentesaux D, Prabhu V (2015) Sustainability in manufacturing operations scheduling: a state of the art review. *J Manuf Syst* 37:126–140. <https://doi.org/10.1016/j.jmsy.2015.08.002>
76. He W, Xu L (2015) A state-of-the-art survey of cloud manufacturing. *Int J Comput Integr Manuf* 28:239–250. <https://doi.org/10.1080/0951192X.2013.874595>
77. Isaksson AJ, Harjunkoski I, Sand G (2018) The impact of digitalization on the future of control and operations. *Comput Chem Eng* 114:122–129. <https://doi.org/10.1016/j.compchemeng.2017.10.037>
78. Iarovyi S, Mohammed WM, Lobov A, Ferrer BR, Lastra JLM (2016) Cyber-physical systems for open-knowledge-driven manufacturing execution systems. *IEEE Proc* 104:1142–1154. <https://doi.org/10.1109/JPROC.2015.2509498>

79. Mitrea D, Tamas L (2018) Manufacturing execution system specific data analysis-use case with a cobot. Access 6:50245–50259. <https://doi.org/10.1109/ACCESS.2018.2869346>
80. Cardin O, Trentesaux D, Thomas A, Castagna P, Berger T, El-Haouzi HB (2017) Coupling predictive scheduling and reactive control in manufacturing hybrid control architectures: state of the art and future challenges. *J Intell Manuf* 28:1503–1517. <https://doi.org/10.1007/s10845-015-1139-0>
81. Zong W, Wu F, Jiang Z (2017) A Markov-based update policy for constantly changing database systems. *Trans Eng Manage* 64:287–300. <https://doi.org/10.1109/TEM.2017.2648516>
82. Gai K, Qiu M, Zhao H, Sun X (2018) Resource management in sustainable cyber-physical systems using heterogeneous cloud computing. *Trans Sustain Comput* 3:60–72. <https://doi.org/10.1109/TSUSC.2017.2723954>
83. Tracy KW (2016) Cloud application sprawl in enterprise applications. *Potentials* 35:26–29. <https://doi.org/10.1109/MPOT.2015.2423690>
84. Yin J, Lu X, Pu C, Wu Z, Chen H (2015) JTangCSB: a cloud service bus for cloud and enterprise application integration. *Internet Comput* 19:35–43. <https://doi.org/10.1109/MIC.2014.62>
85. Gallardo G, Hernantes J, Serrano N (2018) Designing SaaS for enterprise adoption based on task, company, and value-chain context. *Internet Comput* 22:37–45. <https://doi.org/10.1109/MIC.2018.043051463>
86. Hwang J (2016) Toward beneficial transformation of enterprise workloads to hybrid clouds. *Trans Netw Serv Manage* 13:295–307. <https://doi.org/10.1109/TNSM.2016.2541120>
87. Gupta S, Misra SC (2016) Moderating effect of compliance, network, and security on the critical success factors in the implementation of cloud ERP. *Trans Cloud Comput* 4:440–451. <https://doi.org/10.1109/TCC.2016.2617365>
88. Bonino D, De Russis L, Corno F, Ferrero G (2014) JEERP: energy-aware enterprise resource planning. *IT Prof* 16:50–56. <https://doi.org/10.1109/MITP.2013.22>
89. Tarafdar M, Beath CM, Ross JW (2017) Enterprise cognitive computing applications: opportunities and challenges. *IT Prof* 19:21–27. <https://doi.org/10.1109/MITP.2017.3051321>

**Part III**  
**Connectivity and Novel Technologies**

# Chapter 7

## Blockchain Mechanisms as Security-Enabler for Industrial IoT Applications



**J. Rian Leevinson, V. Vijayaraghavan and Muthu Dammodaran**

**Abstract** The introduction and enactment of Industrial Internet of Things (IIoT) have initiated a global revolution. The volume and variety of data that are collected and processed in industries are ever increasing due to the widespread acceptance of modern technologies such as Internet of Things (IoT), big data analytics, machine-to-machine (M2M) communication, edge computing, and cloud storage. Conventional systems with centralized architecture are not designed to handle the complexity and scale of data that is processed in IIoT operations. Moreover, the threat of security and privacy breaches also increases with the growth of IIoT-connected devices. IoT devices often tend to have poor security defense systems due to low processing power, limited storage capabilities, and poor manufacturing standards. In this context, blockchain technology can help to eliminate the security vulnerabilities faced by the IIoT systems and provides extensive protection from data thefts, cyberattacks, and data corruption. Blockchain with its distributed architecture offers peer-to-peer networking and enables auditable and transparent transactions. This chapter explores the concept of IIoT and its limitations, and the need for deploying blockchain mechanisms in the IIoT paradigm. We further analyze blockchain technology and how it can reinforce IIoT systems. Existing systems of blockchain in the IIoT ecosystems and relevant use cases are also explored. As conventional systems struggle to handle the scale of data operations handled by the IIoT, blockchain has emerged as a viable solution to reinforce and reform existing systems.

**Keywords** IIoT · I4.0 · Industry 4.0 · Blockchain · Cybersecurity · Supply chain · Data privacy · Cryptography

---

J. Rian Leevinson  
Infosys Limited, Chennai, India  
e-mail: [rian.leevinson@infosys.com](mailto:rian.leevinson@infosys.com)

V. Vijayaraghavan (✉) · M. Dammodaran  
Infosys Limited, Bangalore, India  
e-mail: [Vijayaraghavan\\_V01@infosys.com](mailto:Vijayaraghavan_V01@infosys.com)

M. Dammodaran  
e-mail: [dammodaran.muthu@infosys.com](mailto:dammodaran.muthu@infosys.com)

## 7.1 Introduction

The Industrial Internet of Things (IIoT), also known as Industry 4.0 or I4.0, refers to the extension and use of the Internet of things (IoT) in the industrial sector to build interconnected ecosystems. IIoT is used to integrate various machines, systems, actuators, and devices using sensors and IoT gateways so that they can seamlessly collect, process, and exchange data between each other. The introduction of IIoT and its subsequent implementation in the industrial world has completely changed how factories manage their systems and processes. IIoT is also one of the critical factors that drive Industry 4.0 which is considered as the current industrial revolution. This new generation of industries has integrated systems with a centralized architecture where all the systems are interconnected with IIoT. Data is collected using various sensors and it is transmitted to the cloud-based systems where they are stored, processed, and analyzed.

However, the swarm of interconnected devices generate massive volumes of complex data that conventional centralized systems struggle to handle. Security threats and vulnerabilities also tend to increase with the increase in the number of connected devices. Since more and more data is collected, privacy becomes another concern as any breach can compromise confidential information.

Blockchain, being a system of linked records, helps to overcome most of the limitations faced by the IIoT. Since blockchain is resistant to modifications and changes with sophisticated cryptography, it is considered extremely secure. The distributed system is also essential in industries and factories as even if one node fails, the rest of system must continue to function. This is not the case in conventional systems where the failure of the central system can cripple the entire network. Since the blocks in blockchain are secure by design, they offer excellent privacy and safety features. Combined with the IIoT vision, blockchain delivers unparalleled solutions that can empower and revolutionize industrial processes.

The flow of this chapter progresses as follows: Sect. 7.2 introduces the concept of the IoT and the issues faced by current IIoT systems as well as their subsequent impact. Section 7.3 analyzes blockchain technology, explores its features, and explains how blockchain helps to secure IIoT. Section 7.4 explores the architecture of a blockchain-IIoT platform in detail and provides a brief overview of popular blockchain platforms. Section 7.5 explores a few use cases of blockchain in IIoT. The conclusion is presented in Sect. 7.6.

## 7.2 The Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT) refers to the implementation of the IoT in the industrial sectors by integrating and interconnecting various machines and devices. The machines are embedded with electronic sensors, actuators, and other digital devices to collect, process, and store data. IIoT allows efficient and seamless

transmission of data between devices. The implementation of IIoT has led to smart factories, optimized production lines, smart environments, customized manufacturing, and increase in overall efficiency. The widespread acceptance of IIoT-related technologies is one of the major contributing factors to Industry 4.0 which is considered the fourth industrial revolution. This marks a new era in the industrial world which is led by IIoT, cloud computing, big data, and advanced analytics [1].

IIoT technology has been implemented in industries for a variety of uses such as the predictive maintenance, asset tracking, fleet management, warehousing, customized manufacturing, and efficient production lines. It has been used over a wide range of industries such as automobile, logistics, transportation, e-commerce, manufacturing, mining, and shipping [2].

Although IIoT sees widespread usage in the industrial sector, it suffers a variety of critical issues that are similar to those experienced by IoT-based systems. These shortcomings are mainly related to the security aspects, privacy, trust, and interoperability. These issues act as major hindrance toward the full-scale realization and implementation of IIoT technology in industries. Therefore, it is essential that these issues are well understood and appropriate solutions are proposed.

### ***7.2.1 Issues and Limitations of IIoT***

The lack of robust security architecture in IIoT networks renders them susceptible to cyberattacks [3]. This lack of security can be attributed to poor manufacturing standards, lack of interoperability, limited processing capabilities, and small storage capacity. Since industries involve confidential data like the design of new products, assembly procedures, financial, and personal data, an attack proof security model is essential [4]. Moreover, the data is most vulnerable when it is being transferred and IIoT systems lack strong encryption layers due to constraints in computational capabilities.

Privacy is also a major challenge in the IIoT paradigm. Protecting the privacy of the stakeholders by securing the data is essential. Privacy concerns arise primarily due to insufficient security measures in IIoT devices. Data is often transmitted with little or no encryption and can hence be easily misused by anyone who manages to access it. The large number of connected devices also poses a massive challenge to privacy as it is difficult to monitor the integrity and security of all the devices continuously. Moreover, since the devices are placed in remote locations at field sites in industries, they are vulnerable to data leakages and eavesdropping. IIoT devices need privacy by design to cope with global standards and increase adoption rates in industries [5].

System safety and reliability are the highest priority of many OT (Operational Technology) platforms. This means preventing the system and its components from causing unacceptable risk of injury or physical damage, protecting the environment against harm, and avoiding interruption of safety-critical processes. As most OT systems in the past were not networked, security and privacy were not a major concern. With IoT being extensively accepted and implemented, it is fundamentally

transforming this perspective in the industrial world. Networks of IoT devices are used to digitalize conventional OT systems. With the current connection of OT and IT (Information Technology) under IoT, remote attackers exploit the weaknesses in industrial, consumer, and public sector IoT systems to break into the OT system and drive it into an unsafe or unreliable state.

In addition, the employment of remote management that includes reconfiguration and updating of devices as well as monitoring and operational reprogramming is creating serious next-generation security and safety concerns. The introduction of IoT systems with open ports and the potential interjection of malicious code, especially on safety devices and systems such as transport, city public safety, and water are creating new requirements for security and safety that are not currently addressed appropriately.

IIoT systems face issues in integration and interpolation with existing operational systems. These mainly stem from the fact that conventional mechanical and operational systems lack the flexibility to accommodate new additions such as IIoT-based solutions. Moreover, the lack of manufacturing protocols and guidelines has led to the production of IIoT devices that are not interoperable with each other. This remains a key factor in the slow adoption rates of IIoT-based solutions in industries.

IIoT devices are often placed in inaccessible remote locations in industries that render conventional regular maintenance services impractical. This makes reliability a key factor in IIoT systems. Another issue with the placement of IIoT devices in remote locations is the problem of connectivity. IIoT networks may also face communication disruptions and interferences due to their close operational proximity to heavy machines. These disruptions and disconnections could lead to the loss of critical information and may cause system vulnerabilities.

### ***7.2.2 Impact of Attacks on the IIoT***

As modern organizations use IIoT networks to run their processes, they are exposed to a variety of security threats including data leakages, cyberattacks, data theft, dangers related with IT/OT assembly, and insider threats. IIoT ecosystems are especially prone to such attacks due to their poor security standards. If the vulnerability of the network is exploited, potentially catastrophic consequences like theft of critical data, loss of production, crippling the system, and data loss may occur [6].

Conventional mechanical systems store data in physical form or in local storages that provide a considerable amount of security. However, modern systems have huge volumes of sensitive data stored and transmitted online that makes them extremely vulnerable to security threats.

Modern IIoT networks are exposed to a variety of threats and the number of security breaches and exploitations is continuously on the rise. The main types of attacks include brute force attacks, hacked devices and networks, viruses, malware, worms, physical tampering, system assaults, and encryption attacks.

In the recent past, there have been successful attacks on extremely sensitive systems such as atomic power plants, water supply plants, and vehicles. Moreover, investigations have revealed critical vulnerabilities in existing IIoT applications such as medical pacemakers and cars. If such vulnerabilities are exploited, they could have dire consequences and can severely hamper the adoption of IIoT systems across industries.

## 7.3 Blockchain

Blockchain is a distributed transaction ledger that is used to maintain records of transactions and operations. It is a linked chain of blocks that contain the details about the transactions. When a new transaction is performed, a block is created with all the relevant transaction details and then connected with the other blocks. It essentially forms a distributed system that has a high level of interconnection between the transaction blocks unlike conventional blocks that have a central hub-based design.

Since blockchains are distributed and decentralized, exchanges and transactions in blockchain systems can happen without the verification of the central server. Thus, blockchain can altogether reduce server costs (counting the cost of optimization and operation) and alleviate the execution bottlenecks at the focal server [7].

Tampering data in a blockchain network is extremely difficult due to the fact that the blocks are connected with each other and the entire set of blocks has to be altered to change the data in any one block. Moreover, each communication block would be approved by different hubs and exchanges would be checked. In this way, any distortion in the network can be identified effectively [8].

Blockchain allows users to assume a considerable level of anonymity. Transactions are recorded and monitored and their location is registered but the identity of the individual is preserved. Moreover, the user can create multiple identities to evade detection as well. Such a level of anonymity is possible due to the distributed nature of blockchain networks although it is possible to determine the identity of the user by observing network traffic and the public blockchain system [9].

Since all the exchanges performed in blockchain networks are approved and recorded with a timestamp, clients can easily check and verify the integrity of past records by getting to any hub in the respective system. In Bitcoin blockchain, every exchange can be followed to past exchanges iteratively. It enhances the transparency of the information stored in the blockchain and makes it easily verifiable.

### 7.3.1 *Salient Features of Blockchain*

Blockchains are fundamentally different from conventional transaction networks and they have a variety of special features. Their key functionalities include cryptographic



encryption (asymmetric cryptography), hashing, linked blocks, and smart contracts. Due to their distributed nature, nodes can communicate with each other directly without being processed through a central server. This considerably reduces the time taken to process transactions and also improves the reliability of the platform. The system can continue to function even if a few nodes fail. This is not the case in conventional systems where the failure of the central hub can disrupt the entire network.

Direct encrypted transactions enforce privacy and considerably increase the security aspects of the system. Moreover, blockchains possess the advantage of being easily auditable and hence all the historic transactions can be checked and verified [10].

### ***Cryptographic Hash Functions***

Cryptographic hash functions are used in blockchain to mask and secure the data transferred in transactions. Hashing essentially standardizes the data by taking in various outputs, passing them through a mathematical function and giving output in a fixed format. It produces a unique hash value for each input and hence the original data can be easily retrieved. However, it is impossible to infer the input value from only the hash value and is thereby essential in securing the original data.

Hashing functions do not modify the original message and hence there is no data loss. Furthermore, hashing is entirely different even if there is a small alteration in the input. Hashing is an essential component of any blockchain security system and is extensively used in Bitcoin. Hashing is also used to check for integrity of the data [11].

### ***Blockchain Transactions***

A transaction represents an interaction between two parties. In the case of cryptocurrencies, transactions represent transfer of cryptocurrency between blockchain users. These transactions could also refer to the transfer of messages or recording activities [12].

Each block in a blockchain can contain zero or more transactions. For some blockchain implementations, a constant supply of new blocks (even with zero transactions) is critical to maintain the security of the blockchain network; by having a constant supply of new blocks being published, it prevents malicious users from decoding the blockchain and altering the blockchain itself.

### ***Asymmetric Key Cryptography***

Asymmetric key cryptography (public key cryptography) involves the usage of two distinct keys to encode the data. The original message is encrypted using the public key which is openly available to anyone. However, the data can be deciphered only using a private key which is securely shared among the stakeholders.

Asymmetric key cryptography is an essential part of blockchain cybersecurity. It is a key factor in ensuring the integrity of the messages transmitted through the blockchain system and securing various transactions performed through the system

[13]. Moreover, digital signals are used to verify the authenticity of transactions to ensure that the owner of the private key is the one performing the transactions [14].

Since modern IIoT systems tend to have thousands of devices connected together and communicating with each other, conventional cryptographic techniques are not capable of handling them. This establishes the need for advanced blockchain-based public key encryption techniques especially while handling high volumes of client-server interactions [15].

### ***Blockchain Addresses and their Derivation***

Blockchain systems utilize the concept of addresses as placeholders to enable transactions between entities. An address acts like a unique and secure identifier that is used to label and record transactions. Blockchain addresses are created by pushing the public key through cryptographic algorithms. The address essentially adds a checksum to the public key to prevent wrong transactions especially due to typing errors [16].

The addresses are usually generated using ECDSA cryptographic algorithm which enables the user to sign transactions with a private key and verify it using a public key. ECDSA ensures that the authenticity of the user is preserved by letting other users verify the author of the transactions. However, the public key is very long and inconvenient to use. Hence, the address is derived from the public key and is used to perform transactions.

### ***Blocks in the Blockchain***

Blockchain systems are essentially made of a series of blocks that are connected with each other. These blocks are an integral part of the blockchain system as they are the main entities which perform transactions and store relevant data.

Exchanges are added to the blockchain when a distributing hub distributes a block. These blocks contain data that is cryptographically hashed and also contain information about the previous block that enables the connection between them. This system can be used to assess and verify the integrity of the blockchain system by tracing the previous block connections back to the source block. These blocks also enable peer-to-peer data networking and data transmission as there is no centralized block and the system is distributed.

Legitimacy and credibility are guaranteed by ensuring that the exchange is accurately organized and that the exchanges have been cryptographically marked. Hence, the private key is used to decipher the messages received by a block; and the other full hubs will check the legitimacy and credibility of all exchanges in a distributed block [17].

### ***Smart Contracts***

Smart contracts are modern promises/contracts that are coded in a digital form and are governed by a set of rules. In blockchain, smart contracts act as decentralized applications that facilitate the implementation of complex algorithms. These contracts are generally governed by preset logics and mathematical functions to ensure automation of contracts between users [18].

A smart contract is activated by performing an exchange that invokes it. It executes autonomously and consequently in a desirable way on each hub in the system, as per the information that was incorporated into the exchange. They allow transactions to be performed directly and eliminate the involvement of third parties. Smart Contracts can be traced and audited but they are irreversible as making changes in the blockchain is very difficult [19].

### **7.3.2 How Blockchain Secures IIoT**

Blockchain when integrated with an IIoT ecosystem increases the security prospects of the entire system. Blockchain has excellent privacy and security characteristics that are essential in IIoT systems. It is distributed, sealed, repetitive, and secure and thus helps IIoT systems overcome their critical drawbacks. Since blockchains consist of blocks of data that are interconnected and distributed, they are faster and more resilient to attacks as the data is not stored in a central hub; it is spread throughout the network. Besides, blockchains also use strong encryption algorithms and hashing techniques and are hence extremely secure. Blockchain transactions are also transparent and the identity of the users can be easily verified. This prevents malicious users and devices from penetrating and contaminating the blockchain network.

In IIoT environments, large portion of the correspondence is machine-to-machine (M2M) cooperation, with no human mediation at all. In such situations, setting up trust among the partaking machines is a major test that IIoT still has not met broadly. Blockchain improves trust among devices by ensuring the authenticity of the devices and offering extensive cyber protection. Such networks can also proactively detect [20].

Blockchain networks are tamper proof and extremely difficult to alter. This is essential in the case of IIoT devices as any attempt to manipulate or alter the sensor or gadget can be immediately identified and necessary proactive action taken [21]. If the integrity of any device is compromised, it can be safely and swiftly disconnected from the network as blockchain systems have a distributed design. They do not have dependency on any specific node in the network.

A circulated arrangement of record for sharing information over a distributed system enables fast transactions and thus making it almost impossible for the network to shut down as the failure of any one node will have minimal effect on the overall system. Hash-based securities, check of character, and provenance verification are essential in identifying rogue devices and alleviating dangers.

By enabling registration and validation of devices to enroll against the system, blockchain-coordinated IIoT arrangement can enhance the overall framework well-being. Smart contracts also encourage programmed execution of business rationale. In the absence of a focal framework to assault, dangers of system failure due to potential attacks on the central node can be avoided altogether [22].

## 7.4 Platform Architecture for Blockchain in IIoT

In this section, we explore blockchain platform for Industrial Internet of Things (BPIIoT) as proposed by Bahga et al. [23]. The BPIIoT uses distributed architecture, peer to peer network, and secure connectivity for usage in the industrial sector. This network is based on smart contracts that act as agreements between the customers and the manufacturers. These smart contracts are transmitted through the blockchain system and are essential in building trust among the stakeholders. The blockchain platform integrates the shop floor with the cloud and data services, thereby ensuring a distributed system where the data is shared across nodes. This digitalization of the shop floor is achieved through the use of integrated platforms that make modern solutions faster, safer, transparent, and more efficient compared to their conventional counterparts [23]. The IIoT devices attached to the machines enable them to trade information on their tasks and progress to the cloud through the blockchain system. The gadgets also enable machine to machine communication in the IIoT network and hence machines can optimize their run time and tasks accordingly.

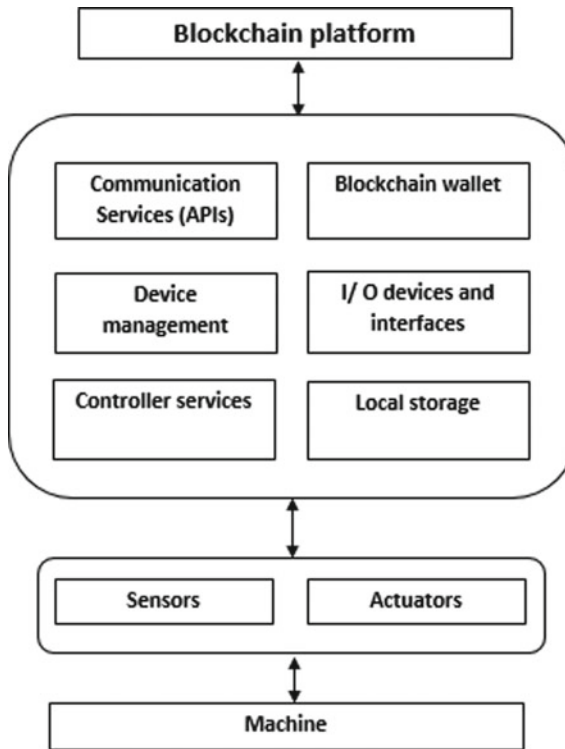
The IIoT devices used in the network primarily consists of two layers: The interface board and a single-board computer (SBC). The interface board has digital and analog I/O functionalities with which the sensors and actuators interact. The interface board and the single-board computer are connected by serial ports and a series of sensors.

The sensors and application drivers are installed in the SBC and they subsequently enable the use of the sensors and actuators to their maximum potential as the drivers are frequently updated and customized according to the current requirements. The SBC can be edited and designed according to the requirements of the user using gadget supervisor present in the SBC. This is possible using a web interface that can also be used to monitor the status of the devices. Moreover, the I/O unit present on the SBC can act as an interface to connect the blockchain-IIoT platform to external networks.

Figure 7.1 depicts the architecture of the proposed blockchain-IIoT system [23] that incorporates an interface board and a single-board PC. Sensors and actuators interact with the interface board that has a sequential interface to the SBC and with the machine. The sensors help establish a connection between the interface board and the SBC and they enable the SBC to receive sensor information from the interface board and send control signs to the actuators.

The blockchain administration on the SBC communicates with the blockchain network by issuing and receiving exchanges to and from the system. Each IIoT gadget has its own record on the blockchain network and maintains a blockchain wallet on the SBC. These records can be easily accessed and their identity can be verified to ensure integrity of the network. The controller administration is used to monitor machine status, working condition, and transmit exchanges to the smart contracts on the blockchain [24].

Figure 7.2 illustrates how users interact with modern industrial systems using the blockchain-IIoT interface [23]. The industrial systems consist of machines and



**Fig. 7.1** Proposed blockchain-IIoT platform

devices that are connected and grouped together to form ensemble applications. The proposed platform is connected to the cloud to store the data and perform analytics. However, the transactions between the user, cloud and the system are processed through the distributed blockchain network which essentially acts as an interconnecting entity. This blockchain offers excellent scalability as more blocks can be added as the network size and number of transactions increase. Furthermore, since blockchains are essentially peer to peer networks, the chain scales with the increase in the number of users.

### **7.4.1 Summary of Other Blockchain-IIoT Platforms**

Although blockchain technology is relatively new, its benefits and applications have been widely realized by organizations and they have developed blockchain platforms in IIoT. These platforms are created by either integrating the technology with an existing IIoT system or developing a new ensemble system altogether from scratch.

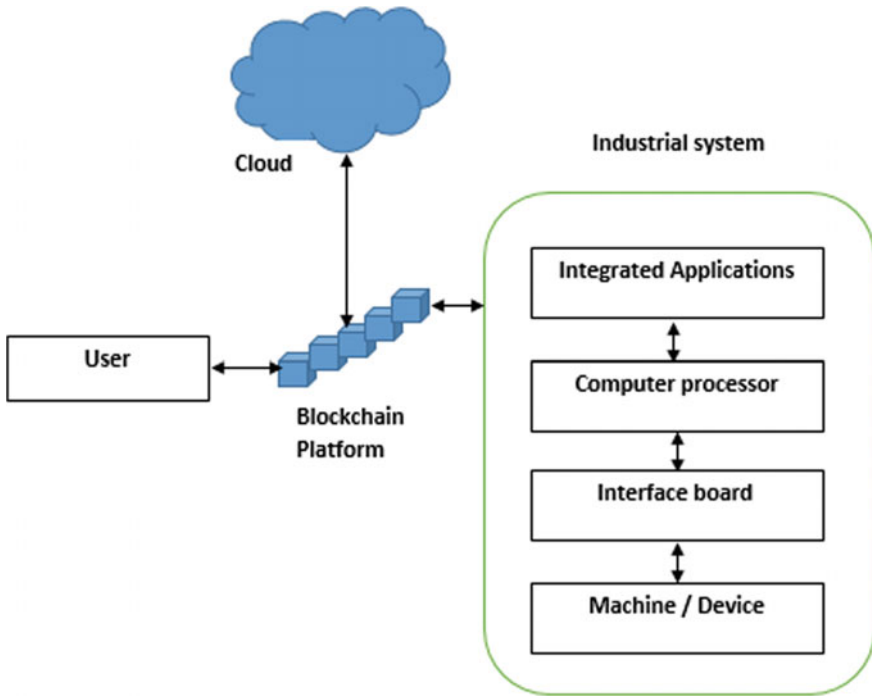


Fig. 7.2 User interaction with blockchain platform

Some of these platforms implemented in the industrial sector are well established, proven, and stable.

The Hyundai digital asset company (HDAC) [25] applies blockchain technology to rapidly and securely transmit data, perform verification and information stockpiling between IoT gadgets. The innovation is connected to industrial facilities and devices to facilitate machine-to-machine exchanges and activity between IoT gadgets. The system consolidates a twofold chain framework (open and private) to build exchange rate and volume, which makes it suitable for IIoT ecosystems. HDAC provides users with the option to select their own transaction fees and allows them to create smart contracts themselves. Moreover, this flexibility is further enhanced by the decentralized approach used by the company in offering IoT data control systems. It also offers transactions through other blockchain systems such as Bitcoin and Ethereum.

VeChain [26] is a global blockchain project that provides IoT-based solutions by ensuring secure collection, management, and exchange of data. The blockchain is utilized in an assortment of routes, with one spotlight being on IoT-based solution in cold chain logistics by utilizing IoT devices to monitor key parameters. Among other applications, the platform can hold car visas by making computerized records of vehicles including fix history, protection, enlistment, and driver conduct all through its lifecycle. Social insurance applications are additionally conceivable by utilizing start to finish following of generation procedures of restorative gadgets; and enable

patients to safely share their biometric information with their specialists to empower constant checking. VeChain [26] utilizes IoT innovation for extravagance merchandize by implanting smart chips in luxury goods for real-time tracking of sales.

Waltonchain [26] is a blockchain platform that is made through a mix of RFID and blockchain advances for successful IoT integration. It is focused on tracing procedures and items in the inventory network. The system involves the concept of merging production line garments, applications, equipment, and managing asset by embedding RFID labels and chips into items. Data with respect to the status of items is then downloaded for examinations onto a protected blockchain.

Ethereum [27] is an open-source blockchain platform that allows user to deploy decentralized and distributed solutions. It uses Ethereum as its crypto currency that is used by miners to pay for transaction fees and services. Ethereum offers excellent support for smart contracts and allows users to create their own applications to perform customized operations. It uses innovative computer software called Ethereum Virtual Machine (EVM) that enables any user to run applications and programs in the blockchain network regardless of the programming language. Ethereum can be used to build decentralized autonomous organizations (DAOs) that are organizations run by software on a system of smart contracts in the blockchain network. DAOs do not have a single leader and are owned by everyone who contributes to it and interact with it by buying tokens. Ethereum is also being used as a secure and reliable platform to launch cryptocurrencies. This is possible, primarily due to the fact that the transactions and digital assets are governed and tracked by special standards such as ERC20 and ERC721. Ethereum is rapidly accelerating the decentralization of the world's economy with its user-friendly, reliable, and secure platform.

## 7.5 Use Cases of Blockchain in IIoT

Blockchain-IIoT integrated systems have already seen a variety of use cases in the industrial world. Organizations have designed, tested, and implemented blockchain and IIoT-based solutions in areas such as transportation, logistics, pharmaceutical industries, and manufacturing factories. This level of acceptance and widespread implementation of blockchain in IIoT systems are primarily due to its unmatched security, transparency, and privacy. This is an especially important factor, provided the volume of sensitive and critical data that modern systems tend to handle.

However, the lack of strong cybersecurity remains one of the major hurdles in the full adoption of IIoT systems. Moreover, industries need auditability and transparency to track and monitor their transactions and this is provided by blockchain. With the integration of blockchain with IIoT systems, organizations are more confident and keener on shifting to such modern systems.

### 7.5.1 Security and Privacy in Supply Chain Management

IIoT and blockchain can push the boundaries of supply chain management (SCM) systems and enhance their operational efficiencies. In modern SCM systems, numerous sensors track key parameters such as temperature, location, vibrations, humidity, level, and orientation of the object, etc. Since these devices share information and communicate with each other, they can use smart blockchain contracts to secure the transmitted data, stored information, and record the transactions performed.

Blockchain systems depend on cryptographic calculations intended to avoid information contortion. Since each block in a blockchain contains a hash to the previous block, it is extremely difficult to alter the chain. Any changes made to a single block have to be done on the entire network and hence, it offers excellent security to the IIoT ecosystem [28].

Figure 7.3 shows an exchange between a purchaser and dealer in a store’s supply chain network [29]. The interaction is processed through the blockchain network and the transmission occurs in the form of smart contracts. The blockchain network contains system information such as the inventory level, purchase order, shipping manifest and invoices. When an input is received, it is matched with the records stored on the blockchain platform and once verified, the transaction is performed.

The need for a viable data sharing method and trust in supply chains fuels the enthusiasm for inventory blockchain networks. Moreover, blockchain networks have enhanced information sharing and security protocols compared to conventional systems [30].

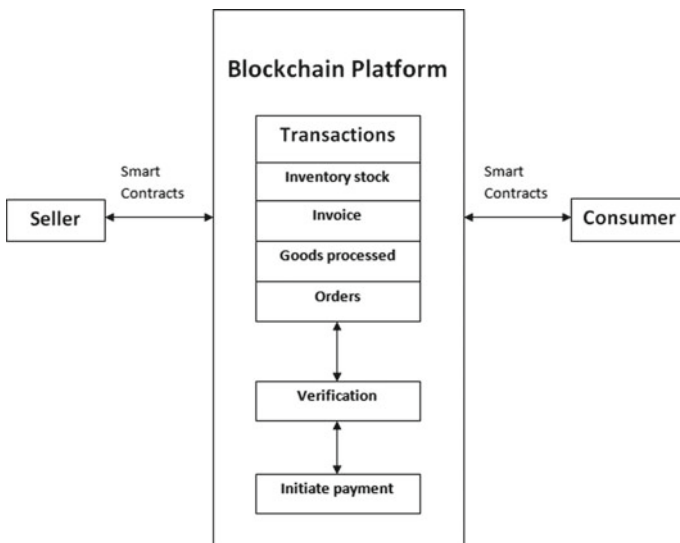


Fig. 7.3 Blockchain in SCM



In blockchain, records are created and stored and they contain information about everything from the stock, source, and destination to the details of the transactions and the entities involved in the transaction.

Stakeholders can view and verify the details of the products at a retailer, such as credibility, quality, quantity, models, reputation of manufacturer, reliability, cost, etc. This also facilitates the continuous monitoring and tracking of shipments throughout their journey. Moreover, due to the distributed nature of blockchains, it is less demanding to access and process data as the data does not have to pass through a central system every time.

The danger of shipment information being adjusted coincidentally or intentionally is a major issue in supply chain systems. Blockchain helps to recognize mistakes or alteration in production network records. Blockchains are extremely resilient to alterations and changes in the network and modifications can be immediately identified. Although blockchain frameworks enable users to view or add information to a record, they cannot alter or erase existing areas in a record. Changes made to records are identified and all the stakeholders are notified with a perpetual log of the changes made.

### ***7.5.2 Pharmaceutical Industry***

The issue of counterfeit medicines in the pharmaceutical sector is increasing with every passing day. The pharmaceutical industry is responsible for developing, manufacturing, and distributing drugs. It is essential to monitor the complete journey of the drugs from the manufacturer to the patient. This is to ensure that counterfeit drugs are not mixed with authentic ones and also to monitor the effectiveness of the drug on the general population. However, this is an extremely difficult task that is often rendered impossible using conventional systems. But the transparent and auditable nature of blockchain technology can help in monitoring the shipment of drugs from its origin to the destination in the supply chain.

Blockchain and IIoT-based systems can be designed to track the legal chain of ownership of prescription medicines. Transparency and traceability are essential when it comes to monitoring sensitive healthcare products. The data stored on the distributed ledger is immutable, time stamped, and secure. This data is accessible by manufacturers, wholesalers, dispensers, and end-customers involved in the supply chain. This ensures that individual drugs can be tracked and monitored throughout their journey using blockchain [31].

### ***7.5.3 Autonomous Vehicle Solutions***

Autonomous vehicles are fitted with thousands of sensors that collect huge volumes of data on the speed of the vehicle, nearby vehicles, pedestrians, wear and tear in

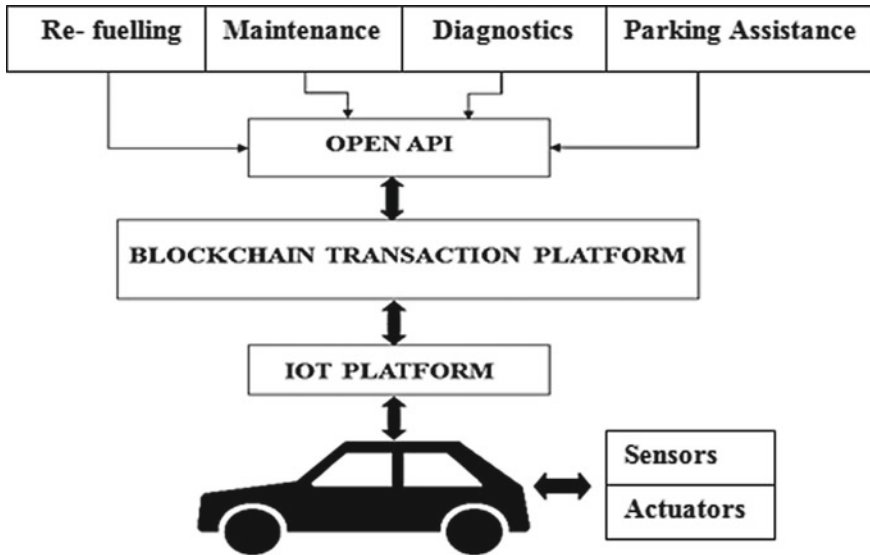


Fig. 7.4 Blockchain-IIoT autonomous vehicle platform

the system, tire grip, proximity to objects, lighting condition, and so on. This data is collected, processed, and analyzed to ensure a smooth driving experience. Figure 7.4 depicts such a system where an autonomous vehicle is embedded with sensors and actuators [32]. The data from the sensors are transmitted to the blockchain network using IoT and is processed to take appropriate decisions.

When the onboard sensors detect anomalies and identify component that could potentially fail, the system can use that information to direct the vehicle to the nearest repair garage. Vehicle manufacturers have plenty of historical data available in the blockchain and this can be utilized for conducting predictive maintenance.

The IIoT layer interacts with the blockchain layer and fetches the appropriate historical data from it, depending on the input from the IoT sensors. Transactions are performed based on this information and are again recorded and stored. This enables data to be stored and accessed in a secure manner and thereby increases the privacy and security protocols in autonomous vehicles.

#### 7.5.4 Manufacturing Process Management

Blockchain and IIoT-based integrated arrangements are used in the production sector to manufacture and assemble mechanical parts and components. Sensors placed in the machinery monitor key metrics such as temperature, pressure, and vibrations and identify deviations from the normal expected behavior. Information received on the blockchain from the sensors is utilized to identify patterns in the anomalous activity

and derive insights from it. This helps in proactively identifying malfunctions and subsequent breakdowns before they actually happen. Such systems are extensively used in the manufacturing of gears where the machine is embedded with multiple sensors that monitor the cut angle, cut depth, temperature, coolant flow, vibrations, and cutting speed.

The information derived from these sensors is transacted through the blockchain system and is subsequently used to monitor the processes. This leads to optimized performance, improved manufacturing quality, and higher reliability throughout the lifetime of the gear. Maintenance workers can monitor the performance of any component in the system by screening the data in the blockchain and can perform preventive maintenance. These observations are also recorded and stored in the blockchain to be used as historical data for further analysis [11].

## 7.6 Conclusion

IIoT facilitates automated and computerized exchange of data, and this data often has sensitive and proprietary information. IoT devices also tend to have poor processing power, very simple architecture, and minimal storage capacities. This causes available resources to be focused on the core functionalities and thereby overlooking security and privacy vulnerabilities. Attackers tend to utilize these vulnerabilities to compromise the security of the system and gain access to confidential data. Conventional security defense systems tend to have centralized security architectures that are computationally expensive, difficult to audit and vulnerable especially as the number of connected devices increases. These issues can be addressed by blockchain with its secure, distributed, and decentralized approach.

Blockchain with its distributed block system ensures that transactions are swift, secure, and private. It provides excellent resilience to attackers as blockchains cannot be tampered or edited. Its continued integration with the IIoT architecture is already leading to significant transformations across multiple industries, bringing new business models and facilitating reconsideration of how existing systems and processes are implemented.

Moreover, blockchain can also be used to transfer information and allocate resources between devices to efficiently control and manage them. Although there are challenges in introducing blockchain into mainstream industries mainly due to computational costs, transaction verification and issues of integration, its future in the IIoT landscape looks extremely promising.

## References

1. Evans PC, Marco A (2016) Industrial Internet: pushing the boundaries of minds and machines. Accessed Jan 2019
2. Zaouini M (2017) Nine challenges of Industry 4.0. <https://iiot-world.com/connected-industry/nine-challenges-of-industry-4-0/>. Accessed Jan 2019
3. Skarmeta AF, Hernández-Ramos JL, Moreno MV (2014) A decentralized approach for security and privacy challenges in the Internet of Things. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp 67–72
4. Atamli AW, Martin A (2014) Threat-based security analysis for the internet of things. In: International workshop on Secure Internet of Things (SIoT). IEEE, pp 35–43
5. Christidis K, Devetsiokiotis M (2016) Blockchains and smart contracts for the Internet of Things. *IEEE Access* 4:2292–2303
6. Das ML (2015) Privacy and security challenges in Internet of Things. *Distrib Comput Internet Technol* 33–48
7. Miraz MH, Ali M (2018) Applications of blockchain technology beyond cryptocurrency. *Ann Emerg Technol Comput (AETiC)* 2(1):1–6
8. Crosby M, Pattanayak P, Verma S, Kalyanaraman V (2016) Blockchain technology: beyond bitcoin. *Appl Innov* 2:6–10
9. Conoscenti M, Vetro A, De Martin JC (2016) Blockchain for the Internet of Things: a systematic literature review. In: IEEE International conference on computer system applications, pp 1–6
10. Kshetri N (2017) Can blockchain strengthen the Internet of Things? *IT Prof* 19(4):68–72 (Article ID 8012302)
11. Wu D, Thames JL, Rosen DW, Schaefer D (2013) Enhancing the product realization process with cloud-based design and manufacturing systems. *J Comput Inf Sci Eng* 13:1–14
12. Skwarek Volker (2017) Blockchains as security-enabler for industrial IoT-applications. *Asia Pac J Innov Entrepreneurship* 11(3):301–311
13. Gross H, Holbl M, Slamanig D, Spreitzer R (2015) Privacy-aware authentication in the Internet of Things. *Cryptography and network security*. Springer International Publishing, pp 32–39
14. Sharma TK (2018) How does blockchain use public key cryptography? <https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography>, Accessed Feb 2019
15. Huh S, Cho S, Kim S (2017) Managing IoT devices using blockchain platform. In: 19th IEEE international conference on Advanced Communications Technology (ICACT 2017), pp 464–467
16. Colombo A et al (2014) Industrial cloud-based cyber-physical systems. *The IMC-AESOP Approach*, Springer, Switzerland
17. Banerjee M, Lee J, Choo KKR (2018) A blockchain future to internet of things security: a position paper. *Dig Commun Netw* 4(3):149–160. Aug 2018
18. Teslya NN, Igor R (2018) Blockchain platforms overview for Industrial IoT purposes. In: FRUCT'22 Proceedings of the 22st conference of open innovations association FRUCT, Article No. 35
19. Luu L, Chu DH, Olickel H, Saxena P, Hobor A (2016) Making smart contracts smarter. In: *Computer and communications security*, Vienna, Austria, ACM, pp 254–269
20. Brody P, Pureswaran V (2014) Device democracy: saving the future of the Internet of Things. IBM. Accessed Jan 2019
21. Miraz DR (2017) Blockchain: technology fundamentals of the trust machine. <https://doi.org/10.13140/rg.2.2.22541.64480/2>
22. Jesus EF (2018) A survey of how to use blockchain to secure Internet of Things and the stalker attack. *Secur Commun Netw* 2018:27, Article ID 9675050
23. Bahga A, Madiseti VK (2016) Blockchain platform for Industrial Internet of Things. *J Softw Eng Appl* 9:533–546
24. Petracek N (2018) Is blockchain the way to save IoT. *Forbes Technology Council*. Accessed Jan 2019

25. Buck J (2017) Bringing blockchain to IoT. <https://cointelegraph.com/news/bringing-blockchain-to-iot>. Accessed Jan 2019
26. Chrisjan P (2018) How significant is blockchain in Internet of Things? <https://cointelegraph.com/news/how-significant-is-blockchain-in-internet-of-things/>. Accessed Feb 2019
27. Ameer R (2017) What is Ethereum? The most comprehensive guide ever! <https://blockgeeks.com/guides/ethereum/>. Accessed Feb 2019
28. Dickson B (2016) Blockchain has the potential to revolutionize the supply chain. Aol Tech, Accessed Jan 2019
29. Rooyen JV (2017) Blockchains for supply chain—part 1. <https://resolvesp.com/blockchains-supply-chains/>. Accessed Jan 2019
30. Kshetri N (2018) Blockchain's roles in meeting key supply chain management objectives. *Int J Inf Manag* 39:80–89
31. Chaudhuri A, Jochumsen ML (2018) Blockchain's impact on supply chain of a pharmaceutical company. In: EUROMA conference 2018, Hungary
32. Laplante PA (2018) Blockchain and the Internet of Things in the industrial sector. Accessed Jan 2019

# Chapter 8

## Visible Light Communications in Industrial Internet of Things (IIoT)



Bugra Turan, Kadir Alpaslan Demir, Burak Soner and Sinem Coleri Ergen

**Abstract** Miniaturization of sensors and hardware for enabling technologies such as wireless charging, energy harvesting, and low-power communications are foreseen to play an important role in the future of various industries ranging from manufacturing to automotive. These industries are projected to become mainly data-driven, as the data acquisition and manipulation capabilities are becoming the main competencies in these industries. Hence, the Industrial Internet of Things (IIoT) emerges not only as a key paradigm for distributed control of actuators but also solidifies the need for capturing and processing data. In this chapter, we discuss the use of visible light communications (VLC) within the IIoT paradigm. VLC considers the use of light sources and photodetectors operating in the visible band of the electromagnetic spectrum (e.g., light-emitting diodes) for communication purposes. Since VLC works in the visible band, it does not further congest the already over-crowded radio frequency (RF) bands. VLC is also secure, RF interference-free, low-cost, and energy efficient. Thus, it has been considered for utilization in many application areas such as intelligent transport systems, indoor localization, and communication in RF-sensitive zones. In this chapter, while discussing the advantages and limitations of using VLC in IIoT systems, we further explore the possible utilization of bi-directional LED to LED communication within this scope for very low-cost communication devices. Finally, we discuss current and possible future applications of VLC in the IIoT context, identifying the following as potential future applications: LED-Based IIoT sensor data transmissions, LED beaconing for localization and signaling, wearable VLC devices for safety, VLC for ubiquitous computing,

---

B. Turan · B. Soner · S. C. Ergen

Department of Electrical and Electronics Engineering, Koc University, 34450 Istanbul, Turkey  
e-mail: [bturan14@ku.edu.tr](mailto:bturan14@ku.edu.tr)

B. Soner

e-mail: [bsoner16@ku.edu.tr](mailto:bsoner16@ku.edu.tr)

S. C. Ergen

e-mail: [sergen@ku.edu.tr](mailto:sergen@ku.edu.tr)

K. A. Demir (✉)

Department of Software Development, Turkish Naval Research Center Command, 34890  
Istanbul, Turkey

e-mail: [kadiralpaslandemir@gmail.com](mailto:kadiralpaslandemir@gmail.com)

© Springer Nature Switzerland AG 2019

Z. Mahmood (ed.), *The Internet of Things in the Industrial Sector*, Computer  
Communications and Networks, [https://doi.org/10.1007/978-3-030-24892-5\\_8](https://doi.org/10.1007/978-3-030-24892-5_8)

VLC-supported augmented reality, VLC for smart farming, VLC-assisted energy load scheduling, VLC-supported industrial Internet of Underwater Things, VLC-offloaded telecom services, and VLC usage in the transportation industry.

**Keywords** Visible light communications · VLC · LED · Radio frequency · VLC Intelligent Transportation Systems · Industrial internet of things · Industrial internet · IIoT · Internet of things · IoT

## 8.1 Introduction

Technology is advancing at an enormous pace. Miniaturization of sensors and further “enabler” technologies such as wireless charging, energy harvesting, and low-power communications are foreseen to play an important role in the future of various industries. Moreover, in the future, different industries ranging from manufacturing to automotive are expected to transform their approaches from a conventional product-driven nature, into a data-driven and environmentally compliant one. As a result, competency in these sectors is expected to be based on data gathering and processing capabilities. Hence, the Industrial Internet of Things (IIoT) is a key paradigm not only for the distributed control actuators but also for more meaningful data capture and processing.

In the context of the IIoT, more refined data directly improve efficiency in terms of serving customers or managing facilities since it enables a more through comprehension of the needs and benefits. However, a massive number of data-capturing IoT sensors are also provisioned to generate new challenges such as infrastructure-independent power (off-grid power) and problems for communications such as spectrum scarcity with contention. Various communication technologies with very low power consumption will pave the way for increasing deployment and penetration of such sensors.

Visible light communication (VLC) is one such communication technology since it is low-cost, energy efficient, secure, and RF interference-free. VLC utilizes light sources such as light-emitting diodes (LEDs) and laser diodes, and optical detectors such as cameras and silicon photodetectors, all operating in the visible light spectrum. Typical setups consist of very low-cost and widely available LEDs modulated via simple driver circuits. These LEDs transmit data to receiver circuits with photodetector or camera front-ends that sense and demodulate the incident light intensity. With the decreasing cost of LEDs and detectors, the simplicity and ubiquity of such components have led to LED-based VLC systems being utilized for many communication tasks in different industrial sectors. Current applications range from automotive, where LED headlights can be used as communication beacons alongside their illumination role, to indoor localization and navigation scenarios, which utilize mobile phones or readily installed infrastructure in large public spaces such as museums and hospitals. LED-Based IIoT sensor data transmissions, LED beaconing for localization and signaling, wearable VLC devices for safety, VLC for

ubiquitous computing, VLC-supported augmented reality, VLC for smart farming, VLC-assisted energy load scheduling, VLC-supported industrial Internet of Underwater Things, VLC-offloaded telecom services, and VLC usage in the transportation industry are just some of the prospective IIoT applications.

In this chapter, we discuss the use of visible light communication in the context of the IIoT. We investigate the advantages and limitations of VLC, utilizing LEDs as transmitters and low-cost photodetectors, cameras, and even solar sensors, as receivers. We further explore the possibilities of the bi-directional LED to LED communication as very low-cost communication devices for IIoT. Finally, we discuss various future application areas of VLC in the IIoT context.

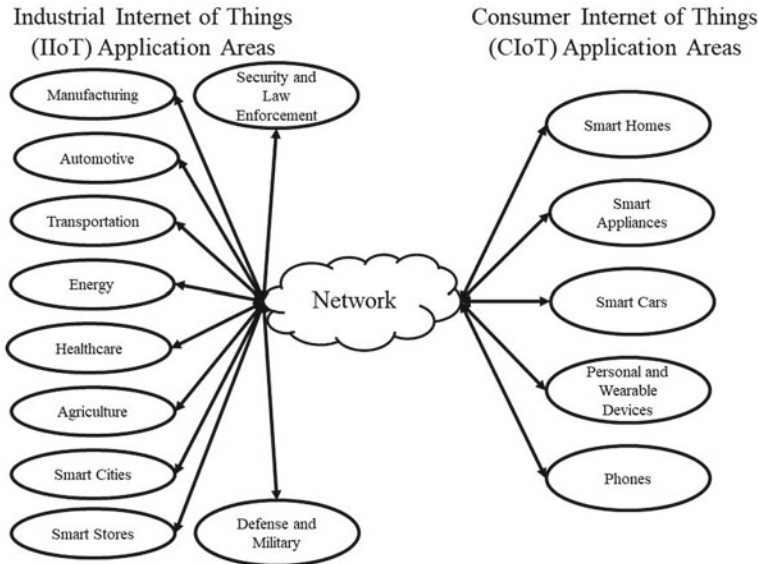
## 8.2 Industrial Internet of Things (IIoT)

The term “Internet of Things” was first introduced by Kevin Ashton in 1999 while he was working on a standard for RFID tagging in logistics applications [1]. Since then, the term and the concept behind the term gained incredible attention. Internet of Things (IoT) may be defined as *an information network of physical objects (sensors, machines, cars, buildings, and other items) that allows interaction and cooperation of these objects to reach common goals* [2]. IoT is also defined as *a paradigm in which objects equipped with sensors, actuators, and processors communicate with each other to serve a meaningful purpose* [3]. The Internet of Things is *the concept of connecting any device to the Internet and to other connected devices. The IoT is a network that connects things and people which collects and shares data about the way they are used and about the environment around them* [8].

Commonly, IoT is divided into two categories based on the application areas: Industrial IoT and consumer IoT. Note that the principles and technologies behind IoT are same whether it is Industrial IoT or consumer IoT. Industrial Internet of Things (IIoT) is the IoT used for industrial purposes. It has many application areas including: manufacturing, transportation, energy, healthcare, agriculture, automotive, smart stores, smart cities, security and law enforcement, and defense and military. Figure 8.1 shows the current and future application areas of the IoT for the industry and consumers. From the figure, it is evident that the application areas for industrial purposes outnumber that for consumer purposes. That is one of the reasons why the IoT is tightly coupled with Industry 4.0 or I4.0 [4–6] or Industrial Internet. The term Industrial Internet is used in North America and Industry 4.0 is common in Europe [1].

The use of IoT devices with embedded sensors in the power grid lines enables the acquisition of real-time data to better manage and distribute energy. The increased availability of real-time data may help to achieve higher levels of energy efficiency. The use of smart devices in transportation, logistics, and connected cars will help to achieve efficiency in terms of energy and environment protection, reduce traffic, and eliminate or decrease accidents. Healthcare and elderly care may benefit from IoT real-time monitoring of people in need. Monitoring of supply chains is an important





**Fig. 8.1** Internet of things application areas

prospective area of IoT use. There is great potential for process efficiency and cost savings via real-time tracking of materials, products, and equipment. IoT provides better monitoring and control of products in smart stores. In the manufacturing sector, IoT may increase efficiency in production, provide better quality control and increased process monitoring.

Internet of Things is not a technology per se, but it is a paradigm for some and a concept for others. Therefore, a number of technologies support the development of the Internet of Things. These are shown in Fig. 8.2. As these technologies and IoT-based applications evolve, the concept of IoT will evolve simultaneously. Moreover, as new application areas are discovered, the dominance of the IoT paradigm will increase.

Smart devices are at the heart of the IoT paradigm. Such devices are composed of embedded sensors, actuators, processing, and communication components. These devices gather data and forward them to other nodes in the networks. The interaction between devices is called machine-to-machine (M2M) communication. The data forwarded to networks are preprocessed, processed, analyzed, acted upon, stored, and recalled at different stages of operation of information technologies. With the right investments and deployments, IoT helps organizations achieve higher levels of efficiency while promising cost reductions.

In Fig. 8.3, a basic IoT architecture is outlined. This architecture is especially suitable for enterprises with a wide area network (WAN) usage. The architecture has three stages. Each stage consists of various devices and fulfills various purposes.

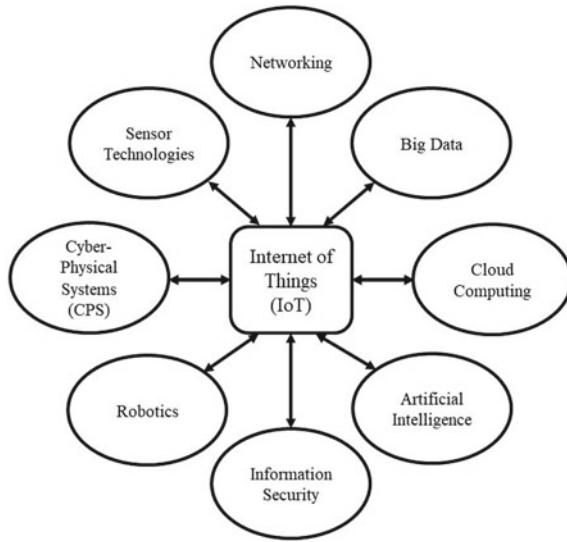


Fig. 8.2 Technologies supporting internet of things (IoT)

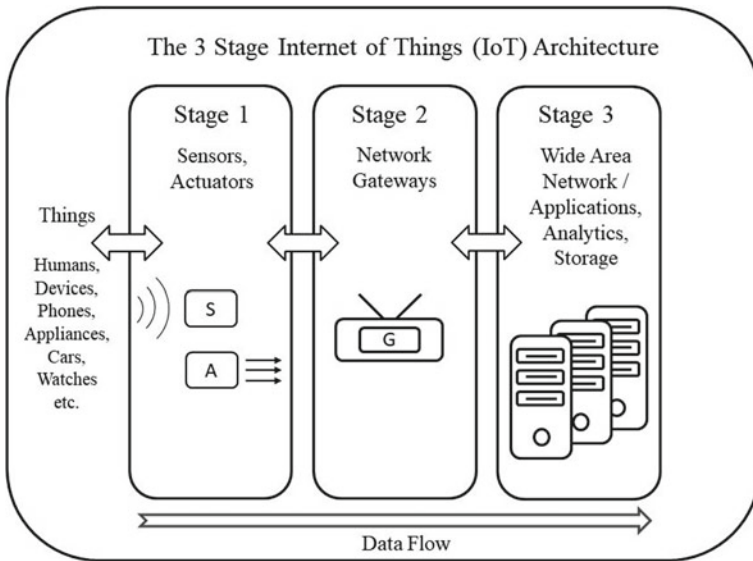


Fig. 8.3 Three-stage IoT solutions architecture

- **Stage 1:** In the first stage, the sensors collect data and actuators conduct various tasks. Depending on the computing capabilities of devices, some level of data processing may also be conducted. The communication component of the devices sends the collected data to a network gateway that may be a part of a network or the Internet.
- **Stage 2:** Network gateways exist in the second stage. The purpose of this stage is forwarding the data collected via sensors and sending the commands to the actuators. The performance of gateways at this stage is important due to the real-time or near-real-time operational requirements imposed by the specific applications.
- **Stage 3:** This is a WAN stage. Here, the data are consumed, analyzed, and stored. Applications make use of the data for various purposes. In addition, the data are stored for in-depth analyses. This stage is where the heavy computation required by the system occurs.

Visible light communication specifically provides solutions to the connectivity between stages 1 and 2. While Fig. 8.3 presents a generic IoT architecture solution for enterprises, and there are also IoT reference architecture models that are either well developed or are in development. Reference Architecture Model Industrie 4.0 (RAMI 4.0), Industrial Internet Reference Architecture (IIRA), Internet of Things Architecture (IoT-A), Standard for an Architectural Framework for the Internet of Things (IoT), and Arrowhead Framework are among these IoT reference architectural models [1]. RAMI 4.0, IIRA, and IoT-A have completed versioned models. IIRA is a US-based effort and the other two have originated from Europe. These reference models provide architectural solutions to relevant industry sectors.

### 8.2.1 IIoT: Current Trends

The Industrial IoT market is estimated to reach \$123.89 Billion by the year 2021 [7]. In 2017, the global IoT market generated a revenue of more than \$57 billion, which is expected to rise at a CAGR of 21% between 2018 and 2023 [7]. Healthcare sector was leading the market with a revenue of \$731 million and is expected to lead again in the following years [7]. Note that while healthcare may be considered an industry, it also affects consumers directly. These numbers indicate a promising future for the IoT both in the industry and daily life. A recent IoT market research and trends forecast report for 2018–2023 [8] highlights certain application areas that are expected to grow in the near future; healthcare, agriculture, logistics, and the energy industry are among these areas.

As the IoT market forecasts indicate, healthcare is one of the most promising industries for the IoT. The investments in IoT in healthcare surpass most other sectors. This is somewhat understandable since health is crucial for all people. There are many patients that are struggling with certain conditions requiring close monitoring. IoT devices may help in monitoring of these people. If emergency conditions occur, the IoT devices may contact necessary healthcare personnel to help the person in

need. IoT devices may also be used in health monitoring of not only ill people but also healthy people. Today, smartphones are equipped with various health sensors. Consumers use mobile health applications when they are doing sports or hiking.

Diseases, insects, and infestations are major concerns for crop yield. IoT may help to address these concerns. Drones may be utilized to patrol large agricultural areas to scan the crops for diseases, insects, and infestations. Drones may take pictures of the crops and send them to computers for image analysis. With such analysis, we may identify the infected crops which may then be removed from the plantation to stop the further spread of infestation. We may also use IoT devices equipped with various sensors to closely monitor the health of the crops and the status of the plantation. The data collected may help increase crop yield.

The logistics industry is another important sector that IoT offers many opportunities to. Secure and timely transportation of goods through the supply chain is at the heart of the logistics business. Supply chain efficiency is also crucial for many businesses. IoT may help in close monitoring of goods in storage and transport. For example, there are many food products that should be kept under certain environmental conditions to prevent them from going bad both in storage and during transport. IoT can help to monitor and maintain these environmental conditions.

IoT offers many opportunities for the energy sector. Real-time monitoring of power lines, increased control over power plants, monitoring the security and safety of pipelines, and smart metering are only a few of the potential applications. With real-time monitoring and data collection, just-in-time maintenance and repair will help to decrease or eliminate power outages. Furthermore, machine learning and data analysis methods coupled with qualified data collection may help to increase energy efficiency.

Improving operational efficiency and increasing collaboration between humans and machines are among the essential drivers of the IIoT market. Tables 8.1 and 8.2 list the components and software segments in the IIoT [7, 8]. Since IoT is not a technology on its own but a paradigm, the developments on the supporting technologies in these

**Table 8.1** Component segments in the global IIoT market

Sensors
Industrial robotics
Distributed control systems (DCS)
Condition monitoring
Camera systems
Smart meters

**Table 8.2** Software segments in the global IIoT market

Product lifecycle management (PLM) systems
Manufacturing execution systems (MES)
SCADA systems
Distribution management systems

segments will shape the future of the IoT use. Furthermore, they will play an important role in the capabilities and limitations of the IoT.

Networking and communication are essential aspects of the IoT. The communication may be wired or wireless. Currently, Wi-Fi is the most popular wireless solution. However, Wi-Fi is a radio-frequency-based wireless communication technology. On the other hand Li-Fi utilizes LED-based optical wireless communications and is expected to either replace or complement Wi-Fi for many application scenarios. We believe a significant portion of these indoor Wi-Fi solutions will be replaced with Li-Fi solutions in the near future due to the number of advantages of Li-Fi over Wi-Fi. In the next sections, we introduce visible light communication (VLC) and discuss the current and future uses of VLC in the IIoT scenario.

### 8.3 Visible Light Communication (VLC)

In this section, we briefly introduce visible light communication technologies. It is essential to overview the unique characteristics of a VLC system to understand its value for the IIoT domain.

VLC transmitters and receivers vary in capability and complexity. Thus, a framework with well-defined VLC transmitter and receiver requirements will pave the way for successful IIoT implementations. Note that almost all of the technologies described here are commercially available. In Fig. 8.4, we present a typical VLC architecture.

VLC uses intensity modulation and direct detection (IM/DD) of optical signals in the visible light spectrum (400–800 THz). Bits are transmitted via LEDs at high frequencies in such a way that the flicker is undetectable by the human eye. VLC does not require heterodyning (i.e., mixing with a local oscillator to up-convert the modulated signal into higher frequencies). Therefore, it is considered to be a low-complexity communication scheme. On the other hand, pre-emphasis and post-emphasis circuits are demonstrated to boost low-cost, low-power VLC systems up to Multi Gbit/s [9] data rates, where RF counterparts targeting low-power applications are only able to provide a few hundred Mbps rates with higher energy consumptions.

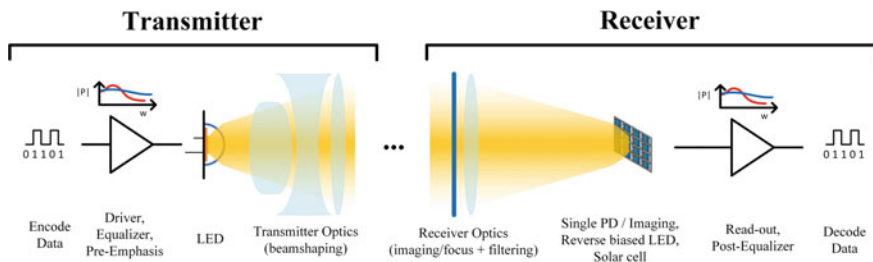


Fig. 8.4 A typical VLC system architecture

### 8.3.1 VLC Transmitters

VLC systems utilize LEDs as transmitters. LEDs are known for their low energy consumption, long lifetime, and low costs. LED optics shape the light beam depending on the illumination needs, providing increased flexibility when compared to halogen or fluorescent light bulbs. LEDs are classified with respect to their manufacturing processes and working principles. Phosphor-coated blue-chips, multi-chips, organic light-emitting diodes (OLEDs), micro-LEDs, resonant cavity LEDs, and quantum dot LEDs (QLED) are the main types of commercially available LEDs. Among these, phosphor-coated blue-chip LEDs (PCLED) are widespread for lighting due to their low cost.

LED modulation bandwidth, defined as the maximum number of on/off state switching times within a second, determines the achievable data rates. As VLC transmitters, phosphor-coated blue-chip LEDs provide modulation bandwidth in the order of a few MHz, due to the relaxation time of the phosphor. Thus, at the receiver side, blue filtering is utilized to capture solely the blue-chip radiation, obtaining 20–50 MHz modulation bandwidths, resulting in higher data rates.

Multi-chip LEDs utilize red, green, and blue chips providing color control depending on the intensities of each chip. Multi-chip white LEDs provide higher modulation bandwidth compared to phosphor-coated white LEDs at the expense of higher costs.

Organic light-emitting diodes (OLED) , as a relatively recent solid-state lighting technology, are also considered as VLC transmitters [10]. OLEDs provide smooth illumination through the panels compared to point source LEDs. However, OLED modulation bandwidth is on the order of a few kHz, limiting high data rate VLC applications. Micro-LEDs and resonant cavity LEDs provide higher modulation bandwidths, and hence, there are higher data rates compared to other LED types. On the other hand, quantum dot LEDs (QLED) provide higher luminous efficiency (i.e., higher optical output with less electric current) [11]. QLEDs are preferred for low-energy targeting applications. Thus, they are mainly deployed on high-resolution television screens and monitors. They provide modulation bandwidths similar to the blue chip with white light illumination.

VLC transmitter LEDs are chosen based on the constraints of illumination, communication range, required data rate, power consumption, and ownership costs. As a result, determining the appropriate VLC transmitter heavily depends on the application area.

### 8.3.2 VLC Receivers

VLC receivers are categorized with respect to their technologies and optical communication requirements. Photodetectors, cameras, LEDs, photomultiplier tubes, and solar cells are demonstrated to be used as VLC receivers.

## Photodetectors

Photodetectors (PD) are the most common receiver types of VLC systems. PDs convert modulated optical signals into electrical current for receiver circuits to demodulate the information. PIN diode and avalanche photodetector (APD) types are employed in VLC depending on the application requirements. APD provides higher gain but also generates more shot noise, whereas PIN diodes have the advantages of low cost, large aperture area, and higher temperature variation tolerances.

## Cameras

Cameras are also used as VLC receivers [12]. They consist of an array of photodetectors. Utilizing cameras as VLC receivers are known as optical camera communications (OCC), a subfield in VLC technologies. A typical OCC system uses cameras (i.e., color image sensor array) to capture incident light signals as image sequence frames. Cameras operate in global-shutter and rolling-shutter modes. In the rolling-shutter mode, captured pixels are sampled row-by-row, where on and off states appear to be light and dark cells respectively. Refer to Fig. 8.5.

In the global shutter mode, all pixels are captured at the same time for the same duration. This mode is favorable for capturing data from mobile VLC transmitters. However, cameras capture a single bit with an image in this mode. Consequently, global-shutter mode provides lower data rates when compared to rolling-shutter mode.

## Light-Emitting Diodes (LEDs)

LEDs work with the same principles as photodiodes. When a positive voltage is applied to the LED cathode, known as reverse-biasing, they act as light receivers. For any LED to be utilized as a VLC receiver, the wavelength of the incoming light should be the same or less than the same LEDs emission wavelength. For example, a yellow color (570–590 nm) emitting LED is sensitive to yellow, green, and blue light, but it will not sense red light since the wavelength of the red color (620–750 nm) is greater than the wavelength of the yellow color.

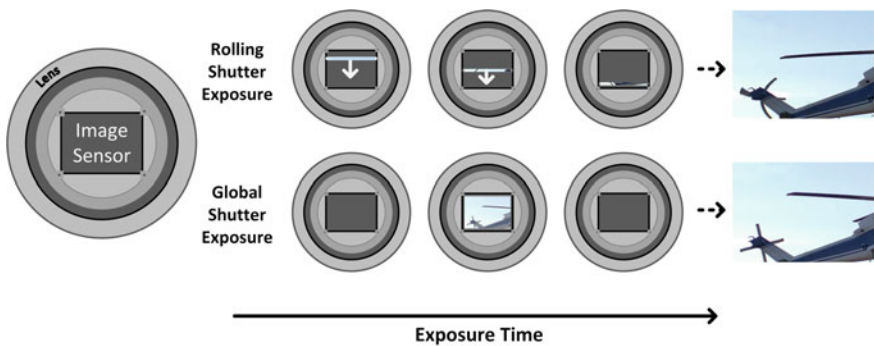


Fig. 8.5 Global shutter versus rolling shutter for OCC

### **Photomultiplier Tubes (PMTs)**

Photomultiplier tubes (PMTs) are another VLC receiver candidates. These enable amplification of a single photoelectron to series of electrons with gains up to 100 million. PMTs are demonstrated to be utilized for weak light detection in extremely dark environments [13], as they are very sensitive to background illumination. PMTs may be utilized to detect non-line-of-sight VLC signals, expanding the use cases of the technology for indoor environments. However, utilizing PMTs for an outdoor environment is challenging due to the increased ambient noise levels from daylight.

### **Energy Harvesting Receivers (Solar Cells)**

Solar cells may be used both as VLC receivers and power supplies for receiver circuits. Transmitted VLC signals comprise of a DC component (converted to electrical energy to charge the receiver electronics) and an AC component which carries the communication signal. Proper receiver electronics enable a few Mbps communication rates and tens of mW of harvested power concurrently with such setups [14]. The dual-purpose of solar cells makes them ideal receiver candidates for IIoT systems with remote distributed units requiring wireless charging and wireless data exchange.

Recently, solar roads are demonstrated to be a viable alternative, generating electricity to supply it to the grid [15]. Thereby, even roads can act as VLC receivers, capturing data from VLC transmitter equipped vehicle LED lights.

## **8.3.3 VLC Advantages**

LEDs use less energy and have a lower cost of ownership than its counterparts such as laser diodes, which also provide optical communication capabilities. LEDs possess additional advantages over other lighting technologies, such as desirable color qualities, minimal or no flicker, long life, and very subtle environmental and human toxicity. The three main benefits of LED lighting are reduced energy consumption, lower cost of ownership, and higher lighting quality. The savings on electricity consumption is also important due to the high consumption of electric power for lighting. Around 6.5% of the total global primary energy was used for lighting in 2005. It is expected that in the USA alone, LEDs will penetrate around 86% of electrical lighting installations by 2035. LEDs will reduce electricity consumption for lighting by around 75% and save approximately 5.1 quadrillion British thermal units (5.1 quads) per year (around US\$52 billion per year) in direct energy costs.

In addition to energy savings, LED usage in the visible light (VL) spectrum for VLC has additional advantages such as unregulated wide spectrum usage. VL spectrum (430–790 THz) is currently unregulated. Therefore, each user can transmit or receive data with the necessary transmit power levels in the spectrum. Moreover, VL spectrum is 10,000 times wider than the RF spectrum (3 kHz–300 GHz).

Future light fixtures ranging from streets [16] to Navy vessels and submarines [17] will all use LEDs, mainly due to their lower energy consumption and higher



lightning quality. However, considering LEDs fast switching capabilities, coupled with a low-cost VLC transceiver circuit, readily available LEDs can serve as VLC transceivers. Thereby, the unused potential of ubiquitous solid-state lighting can be utilized efficiently. On the other hand, as VLC transceiver circuits do not involve complex signal mixing stages, they are free from EMI/EMC considerations. Higher equipment cost is not a concern due to incoherent intensity modulation (IM) transmitter architectures and direct detection (DD) receiver architectures. Moreover, RF-denied environments, such as hospitals, nuclear plants, airplanes, industrial facilities equipped with sensitive electronic equipment, can take advantage of the RF interference/RF radiation-free nature of VLC technologies.

VLC signals cannot penetrate through walls. They are confined to limited areas. Hence, VLC is mainly considered as a line-of-sight (LoS) technology. Such LoS characteristic is useful for information security purposes. It is not easy to hack into the visible light communication outside the line of sight.

Zero energy receivers provide unique advantages to consider VLC in diversified application areas. Utilization of solar cells as the receiver front ends, passive VLC technology, and bi-directional communication abilities of LEDs are among these advantages.

Surveillance cameras have found common use in public and private places. They are used in houses, banks, factories, streets, etc. Each camera may serve as a VLC receiver. This opens up many opportunities for many application areas, especially in IoT applications.

Recently, it has been shown that LEDs cheaper than half a dollar are able to provide 10.2 Gbit/s data rates [18]. This is above the current data rate achievements of the novel fifth generation (5G) communication technologies.

Power-line communications (PLC) provide device connectivity through existing power lines. It has the potential to provide simplified intrabuilding interconnection of devices enabling a cost-effective delivery of broadband data services. PLC systems consist of terminal devices that are plugged into or attached to the electrical power supply network. As LEDs need to be powered via power lines, PLC appears to be an attractive technology for the backbone network of a VLC system, similar to the role Ethernet plays in Wi-Fi-based systems. A VLC modem coupled with a LED front end can receive data from the power line through a PLC modem and then wirelessly transmits the data by optical intensity modulation [19].

Impulsive noise is generated by high-voltage transformers of electric appliances with poor connections. Generally, switching mode power supplies of electronic components are the main source of impulsive noise. RF wireless communications are affected by impulsive noise since the impulsive noise floor created by nearby electronics is usually above the natural thermal noise floor of RF radios. However, optical signals do not interfere with impulsive noise. Hence, impulsive noise does not degrade the performance of VLC systems.

Table 8.3 lists the summary of VLC advantages.

**Table 8.3** Summary of VLC advantages

Energy efficiency
License-free wide spectrum availability
Green technology
Utilization of unused potential
Long LED lifetime
Low-power device utilization
Low-complexity transceiver architecture (IM/DD)
Zero energy receivers via solar cells
RF interference-free—good for RF-denied environments
Increased information security
Same receiver and transmitter architecture (bi-directional LEDs)
Gbit/s (data rates with low-cost devices)
Impulsive noise-free
Easy integration with power-line communications
Readily available cameras as receivers

### 8.3.4 VLC Limitations

Visible light communication is not without limitations. The main barrier being the limited modulation bandwidth. Furthermore, it has some inherent limitations such as nonlinear characteristics of LEDs, being mainly a line-of-sight technology and simultaneous illumination requirement. Currently, the number of market-ready products is low. However, the market is expected to grow as the use expands. We summarized these limitations in Table 8.4.

### 8.3.5 VLC Versus RF Technology: Comparison for IIoT

VLC may be considered as a complementary technology to RF-based solutions for IIoT applications. The most important difference is that VLC features the unregulated and unlicensed optical spectrum where signal reflections depend on the absorption and reflection of light waves. However, RF communications depend on certain spectrum regulations.

Ambient light and background illumination have substantial effects on VLC performance. As VLC transmitters are non-coherent LED sources, they do not produce strong signals for long-distance communications. Thereby, VLC provides only short range and LoS communications. On the other hand, RF communication suffers from electromagnetic interference and noise from the transceivers operating in the same spectrum. RF signals provide longer-distance communications and penetrate through the walls and obstacles.

**Table 8.4** Summary of VLC limitations

Limited LED modulation BW	LEDs are not manufactured for communication. Thus, on and off state switching speeds (modulation BW) are generally in the order of a few MHz
LED nonlinearities	LED voltage/current and optical emission relation is linear only for a limited region. Hence, communication signals requiring high peak to average power ratio (OFDM) do not perform well for all LEDs
LoS technology	Even though non-LoS communications are possible with high-end receivers (avalanche photodetectors, photomultiplier tubes), VLC is generally considered to be an LoS technology
Limited number market-ready VLC devices	Currently, only a few companies have demonstrated market-ready VLC products. Thereby, readily available VLC device costs are high
Illumination for communication	For downlink communication (LED fixture to sensor), illumination is reasonable; however, for uplink communications (from IIoT sensor to receiver), illumination may not be favorable at all times

VLC performance highly depends on receiver aperture size and the selected receiver amplifier. Large aperture size receivers enable a larger field of view with decreased detection capability due to increased noise. However, small aperture area receivers provide higher receiver bandwidths with a limited field of view. VLC receiver amplifiers can be grouped into three, namely, high-impedance, low-impedance, and trans-impedance amplifiers. High-impedance receivers are very low-noise amplifiers, but they provide limited receiver bandwidths. Low-impedance receivers are utilized for high-bandwidth applications where noise is not crucial. Trans-impedance amplifiers provide higher bandwidth with lower added noise.

VLC transmitter radiation pattern is defined not only with LED radiation pattern but also with transmitter optics such as reflectors, lenses, and diffusers. Furthermore, the most common radiation pattern of production LEDs, the Lambertian pattern, asserts that the received optical power not only depends on the transmitter–receiver distance but also depends on incidence and radiation angles.

VLC targets directional communications due to the limited field of view of the receivers. However, RF communications are generally omnidirectional, as they are intended to provide a wide coverage area. VLC, with its shorter wavelengths than RF's, enables efficient spatial diversity schemes to prevent multipath fading, as opposed to the case of its RF counterparts where large fluctuations in received signal magnitude and phase are expected in the link such as deep fading due to constructive and destructive interferences. VLC channels exhibit flat fading characteristics, whereas the RF channel frequency response is oscillatory.

VLC require transmitter and receiver to be aligned. Hence, spatial diversity techniques (i.e., MIMO, MISO) can be utilized to support mobility for VLC. Using high

**Table 8.5** Comparison of VLC and RF communication

Area	VLC	RF
Spectrum range	400 THz	300 GHz
Coverage	Limited	Wide
Security	High	Limited
Licensing	Free	Required
Device complexity	Low	High
Transmitter	LED	Antenna
Receiver	LED, photodetector, camera, PMT	Antenna
Power consumption	Low	High
Mobility support	Medium (using spatial diversity)/low	High
Environment impact	Low	Medium
Channel response	Flat fading	Fluctuating
Market penetration	Low	High

frequencies in the order of THz, VLC does not suffer from Doppler shift, whereas, Doppler shift is a key factor for mobility support in RF systems.

RF technologies are mature enough to be deployed ubiquitously. However, VLC technologies are still in the technology readiness level (TRL) of 6, where research and development efforts are continuing despite a few market-ready products. LEDs global market share is expected to reach 61% by 2020. Considering each LED carries VLC capability, while the technology is considered to be mature, transceiver circuits can be retrofitted to existing LED lighting infrastructure. This will lead to a substantial increase in market penetration.

For RF technologies, antenna gain and patterns are the crucial parameters defining both transmitter and receiver performances. However, various VLC transmitter and receiver types require detailed analysis of application requirements to obtain the desired communication performance.

Refer to Table 8.5 for a comparison of VLC versus RF communication.

### 8.3.6 Future Directions in VLC

In this section, we highlight the further developments and future directions in VL communication.

#### Visible Light Sensing

Visible light sensing applications, such as indoor localization, binary decision/recognition systems for human–computer interaction, and screen–camera communications, rely on the ubiquitous nature of visible light. Visible light is not only

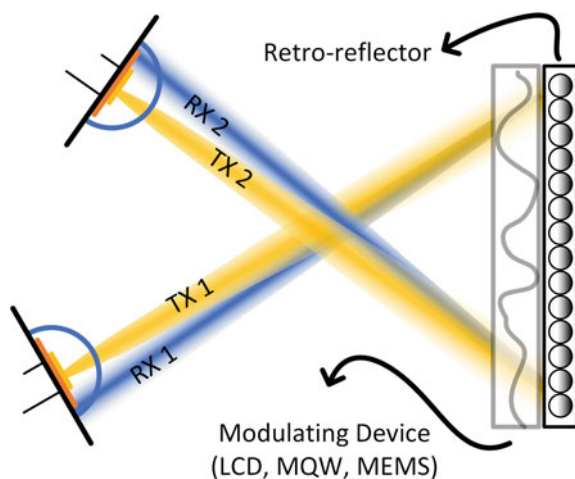
abundant in everyday settings, but its sources are also widely available in man-made devices for utilization in communication and sensing scenarios. Similar to widely adopted Wi-Fi-based localization techniques, indoor visible light positioning systems utilize existing indoor lighting architectures (usually LED ceiling lights) for precise positioning applications [20]. Each LED fixture transmits a unique ID via VLC, where receivers use triangulation via predefined locations of fixtures on indoor maps. Furthermore, visible light sensing applications based on the bi-directional LED usage, where LEDs are utilized as ambient sensors in receive mode, are another appealing direction of VLC utilization [21].

### Passive VLC

Passive VLC [22] aims to modulate the unmodulated light beams of the ubiquitous visible light sources around. Incident unmodulated light beams on the transceiver node are modulated with respect to desired information for transmission. They are, in principle, similar to RF backscatter communication systems that utilize readily available unmodulated nearby RF signals for communication. Such systems are essentially nearly “zero energy transceivers” since they need small amounts of power for operation. As an example, LCD shutters with retroreflectors have proven sub-mW power consumption with ~kbps data rates [23].

The common architecture of retro-reflective passive VLC systems is depicted in Fig. 8.6. Depending on the requirements of the application, other modulators such as multiple quantum wells (MQW) and microelectromechanical systems (MEMS) (i.e., micro-shutters) may also be utilized. The common feature of these modulators is that they modulate the incoming light from the outside, which results in very low power consumption compared to modulators generating their own light (e.g., an LED-based transmitter). This allows the modulating node to be battery-free, which is an extremely desirable feature for IIoT systems with a large number of distributed and remote sensor nodes.

**Fig. 8.6** Passive VLC



## Multi-Gbit/s VLC

Transmitter (LED) and receiver (photodiode, camera, etc.) bandwidth, with VLC channel characteristics, determine the achievable VLC link rates. Even though off-the-shelf LEDs provide data rates in the order of a few hundred Mbit/s, additional systems are required to obtain Gbit/s VLC data rates.

LEDs used for illumination and VLC simultaneously, generally, have a frequency response that resembles a low-pass filter. They exhibit a usable bandwidth below 20 MHz. This low bandwidth puts a hard limit on the data rate since it results in lower optical intensities at higher frequencies for LED optical radiation. Consequently, the signal-to-noise ratios are bad for the higher-frequency signals. To overcome this problem, pre-emphasis and equalizer circuits are used on the LED drivers. These circuits “pump” more power to the LED when higher frequencies are transmitted. For lower frequencies (where the LED response is already good), they simply act as a buffer. Thus, a uniform frequency response is achieved throughout the frequency spectrum (e.g.,  $-3$  dB bandwidth of 400 MHz has already been demonstrated in [24]), allowing for higher-bandwidth light to be extracted from the LED transmitter.

VLC receivers, which usually consist of either a single photodiode or multiple pixels in a camera, also have low-pass frequency response characteristics. Although their typical bandwidth is much higher than LEDs (accessible communication-grade photodiodes typically have  $\sim 100$  MHz bandwidth), they constitute a limitation for achievable data rates. To increase the receiver bandwidth (i.e., flatten the frequency response), post-emphasis/equalization circuits are used.

To achieve Gbit/s data rates, a VLC system needs to be designed with the considerations of VLC channel characteristics. VLC channel models incorporate time and frequency dispersion characteristics of the VLC channel. Once known, the inverse of the channel model can be imposed on the transmitter and receiver to complement the degradations caused by these nonlinear effects of VLC channel. This operation follows the same idea as pre-/post-emphasis applied to transmitters and receivers.

Considering various reflections from nearby objects in the IIoT environments, VLC IIoT channel models should be carefully studied to decide an optimal number of transmitter/receiver deployments with ideal locations.

## Robust Communications Through VLC

Robustness of wireless communication depends on channel characteristics mainly defined through the nearby reflector and scatters, mobility, and resilience to malicious intends such as jamming or spoofing.

Redundancy is one of the key solutions to achieve robustness of wireless communications in case of unexpected disturbances in the channel. For example, in an indoor VLC scenario where ceiling lights are transmitters and a mobile robot with an upward facing photodiode is navigating the room, the LoS requirement between the robot and certain lights may be violated at certain times, and thus breaking the link between the light source acting as the transmitter and the robot. To maintain the communication, there must be at least one other redundant light source acting as a backup. While this is a very simple multi-input multi-output (MIMO) exam-

ple scenario for a controlled indoor environment, similar scenarios exist for outdoor settings and more challenging dynamic situations.

On the other hand, characteristics of RF-based wireless communication channels vary a lot with respect to the frequency range occupied. Reflection versus absorption ratios from objects and scattering and attenuation profiles determine channel characteristics and the achievable data rate. For example, while visible light (EM signal with  $\sim 400\text{--}700$  THz frequency) is not able to penetrate through opaque objects (as this requires a “line of sight” between the transmitter and receiver), a VHF signal (EM signal with  $\sim 30\text{--}300$  MHz frequency) can easily achieve non-LoS communication. Similarly, while a 60-GHz millimeter wave channel suffers great attenuation in air (oxygen absorption), visible light does not suffer as badly.

A robust communication channel with a guaranteed performance in a dynamic environment must be capable of multi-band communication (RF/VLC), switching to the “best one for the current condition.” This requires a robust communication architecture that senses its environment and anticipates the performance degradations on different frequency bands. The communication system should be able to take precautions to maintain connectivity. Building communication systems that are aware of their dynamic environmental conditions require the use of state-of-the-art sensing and classification techniques. Autonomous ground carts (AGC) in a factory are a prime example of such systems. With the use of ultrasonic positioning sensors and multi-dimensional optical sensors such as a LIDAR or cameras, AGC first senses its environment and localizes itself in terms of raw data and later processes and classifies this data with advanced machine learning methods to make decisions on how to autonomously navigate in that environment. A similar approach may be used for IIoT VLC systems where the communication system can be trained with sensor data from real test cases. Then the system learns to choose the best performing communication technology (microwave, millimeter wave, VLC, etc.) for certain environmental conditions.

### **Ultra-Low-Cost VLC**

RF communication schemes employ modulation (amplitude, phase, and frequency) of the EM wave at carrier frequencies to convey information. On the other hand, VLC is based on intensity modulation and direct detection (IM-DD) scheme, where only the intensity of the emitted light wave is modulated. Thus, VLC transceivers do not require any high accurate local oscillators or microwave signal mixer components with sophisticated filters, as it is the case for carrier frequency using RF communication systems. An IM-DD scheme provides both power and cost savings for VLC devices, enabling a wide range of use cases such as machine-to-machine communication between very small remote IIoT sensors and data collectors. In such systems, VLC transceivers can be considered as strong candidates due to their relatively easy miniaturization and low complexity. Furthermore, utilizing bi-directional LEDs is another prominent feature for VLC systems allowing additional miniaturization and size, weight, and power (SWaP) reduction, since it completely eliminated the need for an additional receiver such as a photodetector.

Building low-SWaP embedded systems is one of the most important goals of IIoT systems aiming for massive deployment. Even though a circuitry design associated with LEDs as transmitter and receivers requires substantial differences, medium access control mechanisms such as time-division multiplexing are regarded to be practical schemes for bi-directional ultra-low-cost VLC. With appropriate circuitry using impedance matching, pre-/post-emphasis and equalization, and bi-directional LEDs, ultra-low-cost high data rate VLC systems can be obtained. Demonstration of MIMO capabilities and full-duplex VLC systems using bi-directional LEDs are readily available and well discussed in the literature, e.g., in [25].

### **Machine Learning-Based VLC**

Machine learning methods may be employed to enhance visible light communication system design, especially where the design requires robustness and flexibility under dynamic VLC channel conditions. One example of such a design challenge is overcoming inter-symbol interference in dispersive communication channels. Inter-symbol interference (ISI) causes severe signal degradation and high bit error rates throughout the detection process. To overcome ISI issues, conventional VLC system design uses equalizers to reverse the distortion imposed on the signal by the optical communication channel. Although conventional methods sometimes effectively solve this problem, the solutions are usually suboptimal. Recently, artificial neural networks have been demonstrated to perform better than conventional design methods in this area [26]. It is demonstrated that training the receiver detection algorithms with respect to emitted symbols through LEDs, impairments sourced by channel, and LED nonlinearity can be compensated to achieve higher data rates with low bit error rates.

### **VLC and Li-Fi for IIoT Applications**

VLC is considered to be a point-to-point and unidirectional technology, whereas light fidelity (Li-Fi) denotes the networked and bi-directional optical communication. On the other hand, Li-Fi systems consider the utilization of alternative technologies such as infrared or RF for uplink transmissions. Moreover, Li-Fi supports aggregate use cases, where alternative technologies complement limitations of Li-Fi (i.e., Wi-Fi complements Li-Fi in case of a signal loss due to blockage). Li-Fi consists of the application layer, MAC layer, and physical layer. Currently, the IEEE 802.15.7 standard [27] defines the MAC and physical layer of the Li-Fi. Recently, the IEEE 802.11 light communication task group has been formed to amend the current standard.

Both VLC and Li-Fi technologies should be considered for IIoT depending on the application type. Standardization efforts in the context of optical communication for both VLC and Li-Fi are performed together. Thereby, both technologies are growing together in terms of defining the main implementation details and technological advancements.



## 8.4 VLC Implementations in the IIoT Context

Industrial manufacturing cells are envisioned to require higher flexibility to fulfill individual requirements in the future. Robotic tools supported with artificial intelligence are expected to be networked with low latency. Thus, mobile communication will play an important role in enabling fast modifications in the cells. Manufacturing robots connected wirelessly to the infrastructure will enable abrupt changes in the function of robots during the manufacturing process.

Industrial wireless scenarios require inherent robustness against EMI. There, VLC can be used as a complementary solution to RF technologies to realize uninterrupted wireless communications. However, overcoming the line-of-sight (LoS) limitations of VLC is crucial to provide uninterrupted communications during robot navigation in the industrial site. In this context, spatial diversity techniques are proven to be practical in overcoming LoS blockage problems in industrial environments [28].

Currently, there are very few actual implementations of VLC in the industry. In [29], VLC-based IIoT link design was demonstrated for the first time with industrial field trials. All experiments were held within a  $5\text{ m} \times 5.7\text{ m}$  rectangular area cell located in BMW Company's robot testing facility. The cell is reported to be surrounded by a metal cage that was partially covered with acrylic glass. It should be noted that this cell may be considered as a challenging environment for RF signals due to impulsive noise generated from RF signal reflections. During the trials, an industrial robot (ABB IRB6640-235), equipped with a VLC transceiver, transmitted real-time video/data to the infrastructure while moving at full production speed. The movements of the robot involved picking up a grapppler, grabbing a car part, and moving it to a soldering station with a period of 77 s. It is reported that MJPEG compressed HD video was successfully transmitted at a data rate of 19 Mbit/s with latencies in the order of a few milliseconds.

In the industrial wireless scenario, VLC provides inherent robustness against electromagnetic interference. It is reported that VLC technology worked in a typical industrial site involving spot welding with high currents and flashes of light.

Temperature monitoring is another prominent implementation of VLC in the IIoT context. In the proposed system [30], temperature measurement is complemented with a VLC system to transfer the temperature data for monitoring, storage, and analysis. Temperature data from 200 rooms equipped with 1000 LED transmitters integrated with temperature sensors on 10 floors is captured via a CMOS camera. A Hadoop-based big data platform handles 1.44 million daily data records. The image sensor of the CMOS camera captures different positioned sensors with different independent pixels. As a result, a single camera is able to capture multiple light sources simultaneously. Captured images are analyzed using the lightness and darkness of the light source. Data analysis algorithm extracts a region of interest frame with respect to LED positions, removes the maximum and minimum intensities to calculate the average, sets the threshold taking into account of the background lighting, and decodes ones and zeros to map the temperature readings.

## 8.5 Future Directions in VLC for IIoT Applications

IIoT systems are envisioned to be deployed in factories to increase efficiency, reliability, and safety. In this scenario, machine-to-machine (M2M) communication provides the following:

- Sharing of sensor data such as temperature, illuminance, pressure, humidity, inventory levels, operating conditions, and failure alerts,
- Coordination of multiple production robots for precise timing,
- Cooperation of automated guided carts to guarantee seamless material supply to the production units,
- Prevention of downtime using drones to control station communications, where drones detect the failure in a piece of machinery immediately and inform the central control station,
- Support for augmented reality applications,
- Generation of insightful data about assets, environments, and workers to increase productivity, efficiency, and safety.

M2M communications are realized via wired and/or wireless communication systems. However, considering the cost and mobility of robots, wired systems are non-practical. On the other hand, wireless systems are subject to interference and spectrum congestion limitations considering a massive number of devices in an IIoT environment. Thus, optical wireless communications (OWC) is an appealing solution for LoS high data rate wireless communications. OWC enables simple and low-cost location-based M2M type communication with its RF interference-free nature. As LEDs can be retrofitted into the existing sensors and readily deployed, monitoring cameras can be utilized as receivers. Here, VLC is considered a promising alternative among various OWC solutions.

There is no doubt that IIoT applications will benefit from VLC technology. In the rest of this section, we present a few use cases.

### LED-Based IIoT Sensor Data Transmissions

M2M communication networks within a manufacturing or mining facility may require low data rate communications to transmit sensor information. However, to capture high-resolution data from a vast number of sensors in a confined area require higher update rates. Thus, LED-based communications, providing mainly LoS communications, will pave the way for interference-free communications for massive M2M type communications. On the other hand, RF-based M2M communication schemes are expected to suffer from RF spectrum shortage, contention problems due to large area propagation, and time dispersion signal degradations such as multipath, and scattering [31].

### LED Beaconing for Localization and Signaling

LED luminaires are used in manufacturing and storage facilities because of their lower energy consumptions, superior lighting properties, and longer lifetime characteristics when compared to their halogen and metal-halide counterparts. This readily

available LED technology may be utilized for localization and signaling in manufacturing and storage facilities. An automated mobile cart may exchange identifier data with a LED luminaire broadcasting its own unique identifier. Hence, the mobile cart will localize itself according to the received power strength from the luminaire, whereas the central controller will pinpoint mobile cart location using the cart feedback signal conveyed through the luminaire.

The equipment installed with LEDs may transmit beacon signals asking for a raw material delivery to utilize for production. Thereby, a drone detecting the LED beacon signal with the request or the location will immediately respond and attend to the task without any RF interference from Wi-Fi or cellular signals [32, 33].

### **Wearable VLC Devices for Safety**

Low energy consumption and small form factors of VLC transceivers enable their easy integration into wearable devices. Furthermore, certain industry branches such as mining and construction industries are known to be eager for the utilization of more IIoT sensors aiming for increased workplace safety. Mining sites may utilize VLC technology as wearables in the form of a helmet, broadcasting harmful gas detection, or toxicity information to nearby employees [34]. Moreover, photodetectors are small, low cost, and low-energy devices that can be integrated into wearables as VLC receivers. When integrated into a wearable device and accompanied by an indicator, these devices may be used to warn other employees with the broadcasted information captured via luminaries.

Wireless body area networks (WBAN) is another appealing field to be supported via VLC for enhanced workplace safety. Typically, WBAN collects vital health signs and transmits to central units. Currently, RF-based technologies are foreseen to be utilized for WBANs. However, certain sites such as nuclear plants have highly sensitive electronic equipment prone to electromagnetic interference from RF signals. VLC is a safer alternative solution in these types of sites.

In case of an emergency situation, machinery equipment warning lights can also broadcast information regarding the emergency to be captured via PD-equipped light fixtures. The relevant employee in charge (operator, mechanical/electrical technician, raw material supplier, medical supporters, etc.) will be notified for immediate response.

### **VLC for Ubiquitous Computing**

IIoT devices range from tiny sensors to industrial robots of various sizes. These devices collect and process industrial environment data. However, the storage and computing limitations of IIoT devices with large-scale data analysis requirements necessitate technologies such as cloud, fog, or edge computing, to support prevalent applications [35, 36].

IIoT devices send the pertinent data to the edge layer, where the computations will be performed to reduce network traffic and source data encrypted near the data source (i.e., close to sensors). Reduced data set will be further forwarded to the fog layer, which facilitates the operation of storage and computing between edge and

cloud computing layers. Data will be further transported to the cloud layer enabling big data processing and business intelligence.

Miniaturization and low energy consumption are key to the deployment of IIoT sensors and edge layer computers. Thereby, LEDs as VLC transmitters and solar cells or photodetectors as small form factor low-cost, low-complexity VLC receivers are foreseen to be strong candidates fulfilling IIoT edge computing requirements. In the literature, low energy consuming VLC receivers with moderate data rate transmissions are proposed. Moreover, solar panels can also be employed as zero energy VLC receivers, as they are able to generate energy through direct current of artificial light sources and sun.

### **VLC-Supported Augmented Reality**

Augmented reality applications supplement the real-world experience with virtual information mapped onto real-world objects. One of the prospective uses of augmented reality is to provide guidance for operating or maintaining machinery in the field of manufacturing. Today, a smartphone camera is able to capture text messages transmitted from a LED source [37]. A number of opportunities emerge using these technologies. For example, an employee may virtually tag a piece of machinery with information such as operating tips or last maintenance data using an operation status indicator LED. Another user will access this information using a smartphone camera capturing the indicator LED. Moreover, precise location information obtained through VLC receivers will also play an important role in the realization of VLC-supported augmented reality applications.

### **VLC for Smart Farming**

As the population grows, utilizing arable land in an efficient way, while conserving agricultural resources, becomes even more important for sustainable agriculture. In this case, IIoT sensors based on VLC transceivers may be employed to achieve efficient and sustainable agriculture.

Several features of LED lighting such as spectral control, precise intensity control with dimming, spatial distribution control, and easy integration with other devices are proposed for the next generation of agricultural activities [38]. Spectral components of RGB chip based on white LED lights can be changed with red, green, blue-chip illumination levels, enabling the favorable light dissemination for photosynthesis of plants, enhancing nutritional value. Dimming of LEDs enables adjusting accurate required intensity levels. Moreover, spatial distribution control of LEDs can be attained via optical beamforming that is digital current control of each LED pixel in a LED array or optical shape diffusers.

Easy integration of LED devices with other circuits is another important feature. LEDs do not cause electromagnetic interference and crosstalk like microwave circuit components. More importantly, LEDs do not have any harmful effects on plants. Hence, LED-based sensors have the potential to be used in a wide range of applications from soil monitoring to pivot irrigation. Sensors with energy harvesting capability may gather humidity information on soil and transmit the relevant data to aerial drones or autonomous tractors for precision agriculture. As LEDs do

not require significant power when compared to RF wireless communication sensors, LED-based precision agriculture sensors can be deployed in massive numbers. LED-based VLC transmitters on the crop field may also help autonomous tractors to navigate in centimeter-level accuracy.

### **VLC-Assisted Energy Load Scheduling**

Smart factories have started to utilize renewable energy sources [39]. However, renewable sources provide intermittent energy. Thereby, energy load balancing within a facility will play an important role to make the best use of renewable energy resources. As each light fixture equipped via LED or PD can gather data from the monitoring sensors, it will be possible to optimize the machinery equipment working times, climate control of the facility, and lighting levels depending on the provided energy levels.

### **VLC-Supported Industrial Internet of Underwater Things**

Almost three quarters of the planet's surface are covered with water; and water supports life on Earth. With the help of an underwater IoT system, vital marine environments may be managed by monitoring offshore oil and gas pipelines—while also scouring the seabed for pollutants [40]. Industrial Internet of Underwater Things (IIoUT) applications, relying on transmission of data throughout the ocean, enable a system of roaming autonomous vehicles, and underwater sensors, all communicating with each other and relaying information to networks above the surface. This could be used for a wide range of submarine tasks, from pipeline repair and shipwreck surveys to seismic detection and ecological monitoring (e.g. health of animals). As RF signals do not penetrate into the water and acoustic signals provide very low data rates with high costs, VLC can be considered as an alternative technology to connect underwater nodes with higher data rates, compared to acoustic communications.

### **VLC-Offloaded Telecommunication Services**

Cellular service providers in the telecommunication industry are exploring ways to increase the quality of services and energy efficiencies while decreasing the operational costs. With the introduction of 5G networks, more access points (base stations) will be deployed into dense areas. These access points, known as small cells, can utilize higher RF frequencies with increased transmission power due to higher signal attenuation at higher frequencies. However, recent studies state that the kind of non-ionizing radiation emitted by cellular caused increased cancer risks in laboratory animals [41].

Li-Fi networks, providing last mile solutions to cellular users with the concept of optical attocells, are promising options for secure, reliable, low energy demanding, and high data rate communications. Interference between the indoor and outdoor users is avoided with the employment of optical attocells for indoor environments. Cellular base stations can serve outdoor users with reduced power resulting in more efficient and greener mobile networks.

## VLC in the Transportation Industry

Public transportation sector may benefit from vehicular VL communication technologies (e.g., vehicle-to-infrastructure—V2I—and vehicle-to-vehicle communication—V2V) utilizing readily deployed vehicle LED lights and traffic/street lights. Traffic lights may disseminate time-remaining-for-light-state-change information to approaching vehicles. Then vehicles will be able to capture the disseminated information via photodetectors and adjust their speed as necessary contributing to a more energy efficient and time efficient public transportation. Utilizing traffic lights as the V2I transmitter front-end, additional capital expenditure (CAPEX) costs can be avoided when compared to RF technologies.

The future of the railway industry is also envisioned to utilize smart transportation systems, enabling better passenger experience and augmenting the capacity of the rail networks with reduced lifecycle costs. Railway communication systems are provisioned to be the key to realize Internet of Trains applications [42]. Among various communication schemes, inter-car connectivity is utilized to accelerate the coupling process of two vehicles, named virtual coupling, that improves the dynamic utilization of cars (e.g., empty cars will be left at the nearby stations to be coupled with another busy line). Virtual coupling can avoid deterioration of specific mechanical connectors under the rough vibration and impact conditions in railway operations. Considering high reflection of RF signals in railway usage scenarios, VLC is a promising reliable candidate to support inter-car-train communications for virtual coupling realizations.

Advantages of high data rate communications may further be expanded into off-loading information from vehicles at static scenarios, such as logs for maintenance, functional testing, data driven research and development, etc. In [43], a VLC supported augmented reality application, with user interface for fast and accurate identification of safety and security violations is demonstrated. Considering the vast number of sensors and massive amounts of information recorded by those sensors in newer generation vehicles, it will be possible for vehicle service facilities to diagnose the vehicle through the information transmitted via vehicle LED headlights. This kind of application will remove the need for cable-based diagnosing systems, enabling higher flexibility for the technicians while providing time savings.

## 8.6 Conclusions

The Industrial Internet of Things or Industry 4.0 is considered as the next industrial revolution [5, 6] in that the IoT will positively affect many businesses and industries [44]. Communication and networking are among the main pillars of IoT. Although, technology transformations are not easy, they are inevitable [45]. Currently, many

applications utilize Wi-Fi. However, visible light communications (VLC) is an alternative for many radio frequency (RF) wireless applications.

VLC is a promising technology, providing cost-efficient, reliable, green, and low-complexity solutions. As an appealing alternative wireless communication technology for industrial scenarios, VLC is envisioned to complement readily available RF technologies. On the other hand, it can also open new possibilities where RF technologies are not applicable, such as underwater and applications requiring multi-Gbit/s data rates and low energy. Increased solid-state lighting conversions are envisioned to pave the way for more VLC system deployments. VLC also supports IIoT key requirements such as low power consumption and interference-free communications. Thus, IIoT applications can substantially benefit from VLC. Various companies and research groups are already on the way to exploring and implementing the VLC-based systems [46].

In this chapter, we briefly discussed the IIoT and the current trends. IIoT has many application areas including manufacturing, automotive, transportation, energy, healthcare, agriculture, smart cities, smart stores, security and law enforcement, and defense and military. We provide an introduction to the visible light communications paradigm. We briefly discussed VLC transmitters and receivers including photodetectors, cameras, light-emitting diodes, photomultiplier tubes, and energy harvesting receivers (solar cells). Furthermore, we discussed the VLC advantages and limitations, and also compared VLC with radio frequency communication. We noted that VL sensing, passive VL communications, multi-Gbit/s VLC, robust communication through VLC, ultra-low-cost VLC, machine learning-based VLC are some of the future directions in VLC. While there are many prospects, there are only a few successfully deployed implementations of VLC.

Looking ahead, we identified the following potential future applications: LED-Based IIoT sensor data transmissions, LED beaconing for localization and signaling, wearable VLC devices for safety, VLC for ubiquitous computing, VLC-supported augmented reality, VLC for smart farming, VLC-assisted energy load scheduling, VLC-supported industrial Internet of Underwater Things, VLC-offloaded telecom services, and VLC usage in the transportation industry.

Visible light communication methodologies and frameworks are currently in development. As the technology matures, we anticipate a widespread use of VLC both in the IIoT and in other areas.

**Disclaimer and Acknowledgements** The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of any affiliated organization or government.

## References

1. Weyrich M, Ebert C (2016) Reference architectures for the internet of things. *IEEE Softw* 33(1):112–116

2. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. *Comput Netw* 54(15):2787–2805
3. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. *J Electr Comput Eng*
4. MacDougall W (2014) *Industrie 4.0: smart manufacturing for the future*. Germany Trade & Invest
5. Demir KA, Cicibas H (2017) Industry 5.0 and a Critique of industry 4.0. In: 4th international management information systems conference, Istanbul, Turkey, 17–20 Oct 2017
6. Demir KA, Cicibas H (2018) The next industrial revolution: industry 5.0 and discussions on industry 4.0, industry 4.0 from the management information systems perspectives. Peter Lang Publishing Group
7. Industrial internet of things (IIoT) market analysis—by components (sensors, memory, processors, RFID); by end-use industry (manufacturing, transportation, energy, retail, healthcare, agriculture)—forecast (2016–2021)
8. Industrial internet of things (IIoT) market: by component (transmitter, memory, others); by industry verticals (energy, healthcare, transportation, others); by connectivity (wired, wireless, cellular, others); by geography—forecast (2018–2023)
9. Islim MS, Ferreira RX, He X, Xie E, Videv S, Viola S, Watson S, Bamiedakis N, Penty RV, White IH, Kelly AE, Gu E, Haas H, Dawson MD (2017) Towards 10 Gb/s orthogonal frequency division multiplexing-based visible light communication using a GaN violet micro-LED. *Photonics Res* 5(2):A35–A43
10. Chen H, Xu Z (2018) OLED panel radiation pattern and its impact on VLC channel characteristics. *IEEE Photon J* 10(2):1–10
11. Sadeghi S, Kumar BG, Melikov R, Aria MM, Jalali HB, Nizamoglu S (2018) Quantum dot white LEDs with high luminous efficiency. *Optica* 5(7):793–802
12. Le NT, Hossain MA, Jang YM (2017) A survey of design and implementation for optical camera communication. *Signal Process Image Commun* 53:95–109
13. Liu X, Gong C, Li S, Xu Z (2016) Signal characterization and receiver design for visible light communication under weak illuminance. *IEEE Commun Lett* 20(7):1349–1352
14. Wang Z, Tsonev D, Videv S, Haas H (2015) On the design of a solar-panel receiver for optical wireless communications with simultaneous energy harvesting. *IEEE J Sel Areas Commun* 33(8):1612–1623
15. Dockrill P (2016) The world’s first solar road has opened in France. Retrieved from <https://www.sciencealert.com/the-world-s-first-solar-road-has-opened-in-france>. Accessed on 27 Jan 2019
16. Watson B (2017) From light to bright: San Diego is building the world’s largest municipal internet of things. Retrieved from <https://www.ge.com/reports/light-bright-san-diego-leads-way-future-smart-cities/>. Accessed on 27 Jan 2019
17. Ottman DE (2011) ONR’S TechSolutions creating green ideas that light up ships and submarines. Retrieved From <https://www.onr.navy.mil/Media-Center/Press-Releases/2011/Solid-State-SSL-Techsolutions.aspx>. Accessed on 27 Jan 2019
18. Bian R, Tavakkolnia I, Haas H (2018) 10.2 Gb/s visible light communication with off-the-shelf LEDs. In: 2018 European conference on optical communication (ECOC). IEEE, pp 1–3
19. Ma H, Lampe L, Hranilovic S (2017) Hybrid visible light and power line communication for indoor multiuser downlink. *IEEE/OSA J Opt Commun Netw* 9(8):635–647
20. Jovicic A (2016) Qualcomm lumicast: a high accuracy indoor positioning system based on visible light communication. White Paper, April
21. Incipini L, Belli A, Palma L, Ballicchia M, Pierleoni P (2017) Sensing light with LEDs: performance evaluation for IoT applications. *J Imagin* 3(4):50
22. Wang Q, Zuniga M (2017) Passive sensing and communication using visible light: taxonomy, challenges and opportunities. arXiv preprint [arXiv:1704.01331](https://arxiv.org/abs/1704.01331)
23. Xu X, Shen Y, Yang J, Xu C, Shen G, Chen G, Ni Y (2017) PassiveVLC: enabling practical visible light backscatter communication for battery-free IoT applications. In: Proceedings of the 23rd annual international conference on mobile computing and networking. ACM, pp 180–192



24. Huang X, Wang Z, Shi J, Wang Y, Chi N (2015) 1.6 Gbit/s phosphorescent white LED-based VLC transmission using a cascaded pre-equalization circuit and a differential outputs PIN receiver. *Opt Express* 23(17):22034–22042
25. Li S, Huang B, Xu Z (2017) Experimental MIMO VLC systems using tricolor LED transmitters and receivers. In: *Globecom workshops (GC Wkshps)*, 2017 IEEE, pp 1–6
26. Haigh PA, Ghassemlooy Z, Rajbhandari S, Papakonstantinou I, Popoola W (2014) Visible light communications: 170 Mb/s using an artificial neural network equalizer in a low bandwidth white light configuration. *J Lightwave Technol* 32(9):1807–1813
27. IEEE Standard Association (2011) IEEE Std. for local and metropolitan area networks-Part 15.7: short-range wireless optical communication using visible light. IEEE Computer Society
28. Berenguer PW, Schulz D, Hilt J, Hellwig P, Kleinpeter G, Fischer JK, Jungnickel V (2018) Optical wireless MIMO experiments in an industrial environment. *IEEE J Sel Areas Commun* 36(1):185–193
29. Berenguer PW, Schulz D, Fischer JK, Jungnickel V (2017) Optical wireless communications in industrial production environments. In: *Photonics conference (IPC)*, 2017 IEEE. IEEE, pp 125–126
30. Zhou T, Lee X, Chen L (2018) Temperature monitoring system based on hadoop and VLC. *Procedia Comput Sci* 131:1346–1354
31. Kim CM, Koh SJ (2018) Device management and data transport in IoT networks based on visible light communication. *Sensors* 18(8):2741. <https://doi.org/10.3390/s18082741>
32. Do TH, Yoo M (2016) An in-depth survey of visible light communication based positioning systems. *Sensors* 16(5):678. <https://doi.org/10.3390/s16050678>
33. <https://www.bluejayeindhoven.nl/about-blue-jay/>. Accessed on 5 Jan 2019
34. Ashok Hariharan VM, Parthiban R (2015) MINERPAD: a safety gadget for miners using visible light. In: *3rd international conference on advances in engineering sciences & applied mathematics, ICAESAM'2015*
35. Fujimoto N, Mochizuki H (2013) 477 Mbit/s visible light transmission based on OOK-NRZ modulation using a single commercially available visible LED and a practical LED driver with a pre-emphasis circuit. In: *The National fiber optic engineers conference*. Optical Society of America, ppJTh2A–73. <https://doi.org/10.1364/nfoec.2013.jth2a.73>
36. Computing F (2015) The internet of things: extend the cloud to where the things are. Cisco White Paper. Retrieved from [https://www.cisco.com/c/dam/en\\_us/solutions/trends/iot/docs/computing-overview.pdf](https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf). Accessed on 27 Jan 2019
37. Cahyadi WA, Kim YH, Chung YH, Ahn CJ (2016) Mobile phone camera-based indoor visible light communications with rotation compensation. *IEEE Photon J* 8(2):1–8
38. Pattison PM, Tsao JY, Brainard GC, Bugbee B (2018) LEDs for photons, physiology, and food. *Nature* 563(7732):493
39. Micu A (2017) BMW pledges to 100% renewable power by 2020, at COP23. Retrieved from <https://www.zmescience.com/science/bmw-bonn-renewable-pledge/>. Accessed on 27 Jan 2019
40. Kao CC, Lin YS, Wu GD, Huang CJ (2017) A comprehensive study on the internet of underwater things: applications, challenges, and channel models. *Sensors* 17(7):1477
41. Schmidt C (2018) New studies link cell phone radiation with cancer. Retrieved from <https://www.scientificamerican.com/article/new-studies-link-cell-phone-radiation-with-cancer/>. Accessed on 27 Jan 2019
42. Fraga-Lamas P, Fernández-Caramés TM, Castedo L (2017) Towards the internet of smart trains: a review on industrial IoT-connected railways. *Sensors* 17(6):1457
43. Verkamp M (2018) Automotive functional safety and cybersecurity platform. Retrieved from <https://blog.lhpes.com/cyber-security-demonstration-at-iotswc>. Accessed on 27 Jan 2019
44. Demir KA, Turan B, Onel T, Ekin T, Demir S (2019) Ambient intelligence in business environments and internet of things transformation guidelines. In: Mahmood Z (eds) *Guide to ambient intelligence in the IoT environment—principles, technologies and applications*. Springer International Publishing

45. Cicibas H, Demir KA (2016) Integrating internet of things (IoT) into enterprises: socio-technical issues and guidelines. *Yönetim Bilişim Sist Derg* 1(3):105–117
46. Karunatilaka D, Zafar F, Kalavally V, Parthiban R (2015) LED-based indoor visible light communications: state of the art. *IEEE Commun Surv Tutor* 17(3):1649–1678. <https://doi.org/10.1109/COMST.2015.2417576>

# Chapter 9

## The Internet of Things LoRaWAN Technologies in Academia: A Case Study



Lucio A. Rocha, Fernando Barreto and Laio O. Seman

**Abstract** Universities are a propitious place to leverage knowledge and bring life to new technologies to enhance their effectiveness when used in the industry. Universities are a special case of non-profit organizations that offer improvements in teaching, research, and extension activities for their academic community. It is a fact that many companies now partner with academia to evaluate new products, perform internal personnel training, and improve the quality of their production for end markets. In this book chapter, we discuss how to connect cloud services to thousands of IoT end devices with low-range technologies. This chapter consists of an explanation about the implementation of a complete and functional low-power long-range wide area network (LoRaWAN) using the current local wireless infrastructures. Our objective is to report the core aspects to be considered for learning about low-power long-range WAN IoT technologies. These aspects include the analysis of the coverage area, communication restrictions, network data-link and bandwidth, and many others. We also present a set of experiments carried out at a Brazilian university that currently uses novel LoRaWAN technologies and related devices as teaching tools. We enumerate many real possibilities of application of IoT sensing for smart cities with interesting experimental evaluations.

**Keywords** IoT · LoRaWAN · LoRa · WAN · TTN · Long range · Low-power devices · Wireless · Cloud computing

---

L. A. Rocha (✉) · F. Barreto · L. O. Seman  
Computer Systems Research Group, Department of Computer Engineering,  
Federal University of Technology—Paraná, Apucarana, PR, Brazil  
e-mail: [luciorocha@utfpr.edu.br](mailto:luciorocha@utfpr.edu.br)

F. Barreto  
e-mail: [fbarreto@utfpr.edu.br](mailto:fbarreto@utfpr.edu.br)

L. O. Seman  
e-mail: [laioseman@utfpr.edu.br](mailto:laioseman@utfpr.edu.br)

## 9.1 Introduction

Many industries have an interest in establishing partnerships with academia with a view to researching and improving the quality of their production. In this context, academia is a prone place for teaching, research, and extension activities for the academic community, where new technologies may be evaluated before being adopted.

Ankrah and AL-Tabbaa [1] argue that the partnership between academia and industry may be perceived as an enhancement of innovation through knowledge exchange. Many universities encourage the formation of junior enterprises as extension activities for learning about entrepreneurship, consulting, cooperative research projects, employee training programs, and many others. It is essential to foster alternatives to bring new possibilities of research to academia and reduce risks when introducing new products to the industry and end markets.

In the current research, we are interested in exploring how one may learn about long-range wireless technologies in academia with real possibilities of their employment in industrial sectors. Before discussing how such novel technologies may be employed, it is important to consider their inherent characteristics and motives for usage. Long-range wireless may be employed to send/receive small-sized data from thousands of end devices without interference among them, and with low consumption. Conventional wireless, as well as mobile 4G and LTE networks for data transmission have high energy demands. Other technologies such as IEEE 802.11 (Wi-Fi) have low ranges of just a few meters. Currently, there are several motives to use low power consumption and long-range transmission technologies [2] including the following:

- Low consumption powered by very long-life batteries;
- Network devices that communicate with low frequencies and reduced amounts of network data;
- Low data transfer where data packets ranging in size from 10 to 1 KB allow optimized speeds ranging from 3 to 375 kbps [3, 4];
- Wide wireless ranges from 1 km in urban areas to 10 km in open areas. In this sense, it is possible to send small data at longer distances than other wireless technologies;
- Device modules can run with a maximum power of up to 120 MW, e.g., LoRa1276 and related;
- High sensitivity ( $-168$  dB) combined with low interference [5];
- Modules that generally run in non-commercial frequencies, e.g., 100–1050 MHz.

Low-power wide area (LPWA) is a wireless IoT connectivity family of network [4]. Here, LPWA devices communication can reach dozens of kilometers with low power consumption with a single battery pack [6]. This technology is relatively new but is being used widely with many other names in the literature [7], e.g., Internet of Things (IoT). Its characteristics provide motives for use and development of products in this field. Literature highlights markets for ubiquitous solutions, but there are

numerous challenges in using long-range technologies. Such challenges are due to the early development stages of the technologies and lack of standardization. In this book chapter, we present considerations about how to provide a functional long-range infrastructure without interference and using a conventional wireless LoRaWAN infrastructure implemented in one particular university in Brazil.

The rest of this chapter is structured as follows: Sect. 9.2 presents an overview of long-range (LoRa) technologies; Sect. 9.3 is about the many applications of LoRa in the industry; Sect. 9.4 discusses the methodology for implementing a complete and functional LoRaWAN infrastructure in a university; and, finally, Sect. 9.5 concludes the chapter with a summary.

## 9.2 Long-Range (LoRa) Technologies

In this section, we provide a brief explanation about the most recent technologies for long-range wireless communication, and about LoRaWAN specifications to support connections by low-power end devices.

### 9.2.1 Background

Long range (LoRa) [8] is a physical layer wireless communication technology that uses industrial, scientific, and medical (ISM) radio frequency bands to transmit data at long ranges with low power consumption. The modulation is done using the spreading spectrum technique, which can be immune to interference. LoRa is presented in two parts:

- LoRa physical layer: which generates the modulation and has the hardware: the modem or radio using license-free radio frequency bands [5].
- LoRaWAN protocol: which is the network protocol that allows connections of LoRa devices [9–11]. This is a MAC layer protocol and system architecture design added to standardize and extend the LoRa physical communication layer in networks [6, 12].

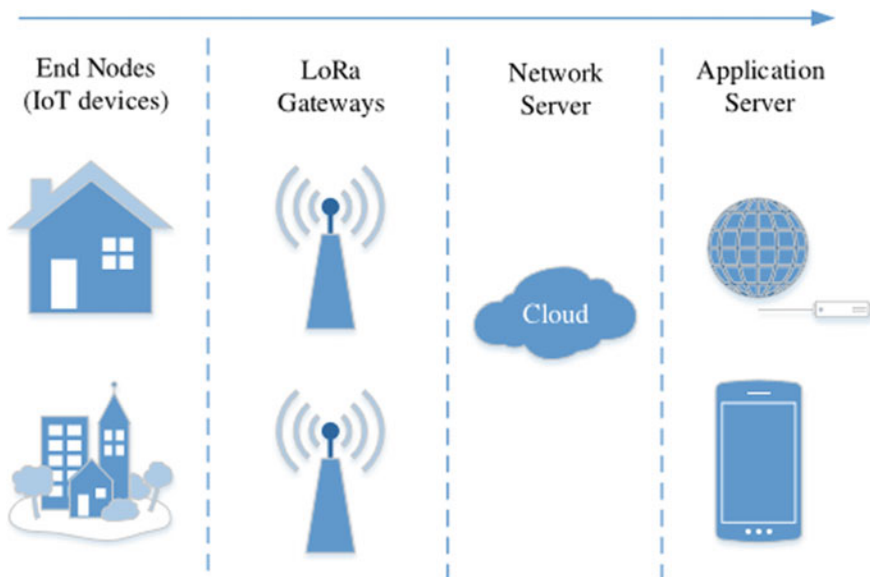
LoRa technology was invented in 2010 by French startup Cycleo, later acquired in 2012 by a semiconductor company Semtech [6]. Currently, LoRa is a proprietary solution owned by the Semtech enterprise and associates. On the other hand, LoRa Alliance is a consortium that develops the LoRa specification and provides LoRaWAN as an open protocol. The infrastructure for supporting many low-power IoT devices is known as low-power wide area network (LPWAN). Other technologies may be used in LPWANs, such as SigFox, Ingenu, LoRaWAN, 3GPP, and weightless. Additionally, LoRaWAN is a long-range wireless protocol for building IoT LPWANs with LoRa technologies. LoRa, Sigfox, and 6LoWPAN are the major protocols for IoT narrow-band communication [9].

There are other technologies that provide long-range communication with low power consumption, most offering proprietary protocols, e.g., LTE-MTC (machine type communications) [13], ultra narrow band (UNB) [14], weightless [15], and R-FDMA [16]. These closed protocols are more susceptible to interference on their radio signals, and most of them use a personal gateway as the entry point. Some of these perform transmission without gateways, such as the csLPWAN [17].

Figure 9.1 shows the components of a typical LoRaWAN network infrastructure. In this network, end-nodes have sensors and/or actuators and use a single-hop LoRa protocol or frequency-shift keying (FSK) modulation to send and receive data with the LoRa gateway in bidirectional communication (uplink/downlink) [6]. These LoRa gateways forward data using IP protocol through the Internet. This mechanism may use a SemTech packet-forwarding protocol (UDP) or a TTN gateway connector (MQTT/TCP). The forwarded data are received and processed by network servers in a cloud environment which offers application servers access to them. The application servers are Web applications for users to access the data from network servers.

Figure 9.2 shows that one end-node can communicate with many gateways in the coverage area. The network server will receive all the messages but, if an acknowledgment message is needed, the network server will deliver it through the best gateway near the end-node (with the best RSSI).

Moreover, the end-devices can use different channels and data rates to send/receive data to/from a gateway without interference among end-devices. LoRa data rates are many times slower than conventional Internet connections, reaching a little over 50 kbps for each device using an adaptive data rate (ADR) scheme. These end-



**Fig. 9.1** LoraWAN network

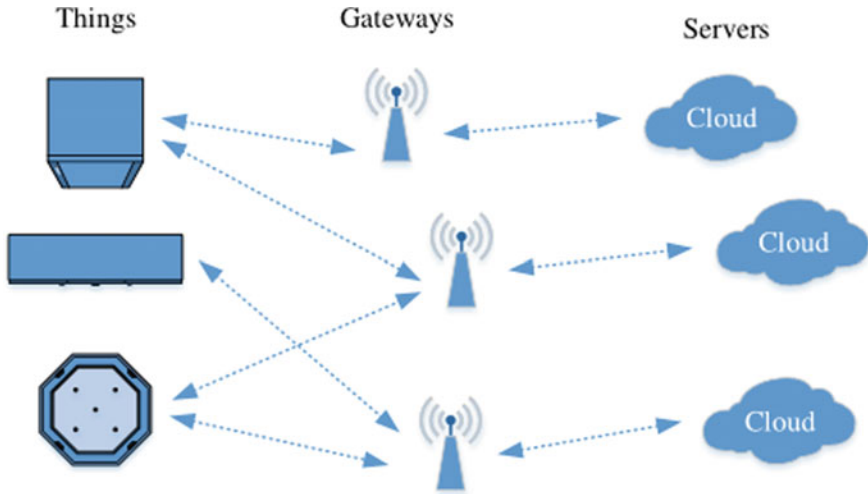


Fig. 9.2 LoRaWAN network with IoT end-devices

devices can use any data rate and/or channel available, without interference among data transfers.

It is important for any LPWAN to incorporate appropriate security. LoRaWAN provides it through two simple layers of security: one for the network and the other for the application. The network security layer ensures the authentication of the node with the network server, while the application security layer ensures the network operator does not have access to the end user’s application data [8]. Both employ symmetric cryptography and registered session keys. There are two types of end-node authentication: activation-by-personalization (ABP) and over-the-air (OTA). ABP uses an explicit key configured in the end-node and network server. OTA performs a JOIN procedure with the network server to negotiate session security keys. The network server (during the JOIN stage) acts as a communication filter, only allowing the transfer of data from end-devices with valid registered keys [18].

The LoRa Alliance [19] offers a global partnership among commercial enterprises, such as IBM [20], Semtech [21], Actility [22], Gemalto [5], Microchip [23], and Cisco [24], and non-profit organizations. The LoRa Alliance seeks to establish a certification and compliance program to ensure interoperability for large-scale network wireless coverage. LoRa devices run on non-licensed ISM radio frequency bands. An appropriate frequency plan must follow the specific country’s regulations. In different regions of the world, the frequency bands are defined by International Radio Regulations, which have divided the world into three regions of the radio spectrum [5]: (a) region 1 covers Europe, Africa, the former Soviet Union, Mongolia, and the Middle East west of the Persian Gulf; (b) region 2 comprises the Americas, Greenland, and the eastern Pacific Islands; and (c) region 3 covers most of Asia, east of Iran, and most of Oceania.

An important note about the frequency regulation for LoRaWAN is that some countries require the registering acquisitions of gateways and licenses. A complete reference about frequency plans and regulations by country is available in reference [25]. The Lora Alliance site [26] presents some modifications according to the region. In Brazil, for example, the frequency regulated by governmental decree [27] is from 915 to 928 MHz. Such frequency bands are the same as the Australian plan (AU915). However, some cloud network services that host IoT devices may change some of these frequencies. An example is The Things Network cloud service, which changed some uplink/downlink bands from the original Brazilian frequency plans, thus requiring some adaptation in end-node programming.

The Things Network (TTN) is an example of open cloud service for IoT devices that provides connectivity for LoRaWAN applications and allows registered devices to send data among them; which is then accessible through the Internet. A gateway is a physical machine that forwards packets from end devices to the TTN through the Internet. Gateways are in the radio coverage of LoRaWAN, but it is necessary to configure them in order to establish connectivity with the TTN. Finally, nodes are registered end devices that have embedded systems which can send/receive data to/from the TTN through the local gateway.

Also, the continuous adoption of the technology has encouraged several recent studies in the literature regarding the modeling of the channel. In [28], the author analyzed the use of time and spatial diversity to enhance the uplink performance in a LoRa network through message replication and multiple receiving antennas, concluding that the adequate combination of both techniques can considerably improve network performance.

The authors of [29] also modeled the channel characterization for wearable LoRaWAN monitors, comprising various operating distances across environments including urban, suburban, and rural areas. Results point to LoRaWAN being a credible wearable wireless technology. On the other hand, results presented in [30] show that collisions among packets modulated with different spreading factors (SF) may cause packet loss if the received interference power is strong enough, thus disproving the common belief that SFs may be considered orthogonal.

Some challenges are also highlighted in [31] for general IoT technologies, including challenges relating to connectivity, efficient energy management, security, complexity, and fast-paced development.

### ***9.2.2 LoRaWAN Specification***

LoRa gateways use classes to define standards implemented by end-devices. At least the basic LoRaWAN class A must be implemented, and, optionally, classes B and C. The composition of such classes is shown in Fig. 9.3. The operations of these classes are defined as follows [6, 8]:



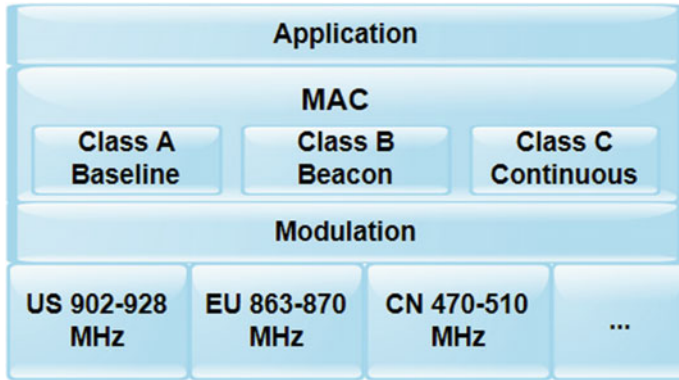


Fig. 9.3 LoRa classes

- Class A (bidirectional end devices): known as the baseline and intended for use in battery-powered sensors. This class of communication is based on an uplink transmission followed by two short downlinks receive windows. It is the lowest power end system for applications that require only downlink communication after using an uplink channel for transmission.
- Class B (bidirectional end devices with scheduled receive slots): this class is intended for use in battery-powered actuators. It uses extra receive windows in predefined scheduled times, in contrast to Class A which openly receives windows at random times. A beacon is used for time synchronization between the end-device and the gateway. This allows the gateway to know when the end-device can receive data.
- Class C (bidirectional end devices with maximal receive slots): this class is intended for use in the main powered actuators with no latency for downlink communication. This class allows end-devices to continuously receive transmission windows, which are only closed when end devices are ready to send data. Although it allows high performance, this class consumes more energy.

### 9.3 Applications in the Industry

According to Ferreira [32], the advent of smart cities comes from the need to solve problems regarding the high urban population increase. There are now emerging possibilities of communication with devices that communicate with each other on the Internet without human intervention. Common terms used for this communication are machine-to-machine (M2M), human-to-machine (H2M), and machine-in-humans (MiH). Most IoT devices follow protocols such as Wi-Fi, Bluetooth, Z-Wave, and RFID for short range wireless communication. For industrial applications, 6LoW-PAN, Z-Wave, and ZigBee protocols are common. Embedded boards are being used

to support the software application in low-cost hardware for many different usages, such as RaspberryPI, BeagleBoard, ESP8266, and similar. However, there is not a common protocol used by most of these devices, and many of them are using two or more communication protocols to avoid connection flaws. Many new protocols are being developed for IoT devices by large organizations such as IEEE, IETF, ITU-T, ETSI, OASIS, and others [32]. Although there is not an agreement about protocols, there is a large set of potential applications for new technologies.

Specifically, in the industry, Navarro-Ortiz et al. [25] affirm that Industry 4.0 is a term used by the German Federal Government to optimize industrial production and provide smart manufacturing solutions. The authors also state that the purpose of the IoT is to increase productivity and reduce environmental impact. Haxhibeqiri et al. [12] evaluate the performance and coverage results for an LPWAN indoor deployment with a single gateway. The authors state that LoRaWAN can cover an entire industrial environment, but metallic apparatus restrict the communication. A simple search in the literature gives many applications. Such applications include smart parking, remote e-health, smart cities, metering, street lighting control, precision agriculture, etc. [33]. Varsier et al. [34] argue that long-range technologies are suitable for non-critical smart metering applications. In [35], the authors measured the performance of LoRaWAN through a long-term deployment of air quality monitoring application, with results showing many insights into the performance. The authors of [36] tested LoRa with an in-soil propagation, showing that LoRa can be a potential technology for wireless ground sensors in underground sensor networks.

In this sense, sensor applications are the most common applications for long-range technologies in cases where conventional wireless communication is poorly offered or not available. According to [22], the penetration performance and deep coverage are very useful features of these technologies. Tens of millions of devices may be used to deliver data to customers or cloud applications hosted by its infrastructure. Ducrot et al. [37] define IoT as a set of interconnected wireless devices that connect and exchange data with each other through protocols, also exchanging information with applications through the Internet. Such devices use many different protocols and produce a very large amount of data in their communications. These authors state that the IoT impacts the business models of many industries and services such as consumer electronics, automotive, utilities, facility management, smart buildings, connected cities, e-health supply chains, and manufacturing.

Many authors also report that connected objects will reach around 10 billion [25] or more than 25 billion connections by 2025 [6]. As an example, these authors state that applications for the industry include increasing security by using monitoring devices, such as gas pressure. Another application is smart parking, reducing the pollution due to looking for a parking spot: LoRa sensors could detect if the parking place is occupied or vacant. Another application is in waste management, to optimize vehicle operations for collecting waste. Large enterprises such as Amazon [38] have invested in the IoT vision as an alternative to optimize the usage of resources in industries and provide more efficiency and productivity.

### 9.4 Methodology to Deploy LoRaWAN

In this section, we describe the methodology used to employ LoRa at the Apucarana campus of the Federal University of Technology, Paraná, Brazil. We discuss the LoRaWAN infrastructure, the registering of IoT end-devices in TTN, and some aspects of security in this methodology. The objective of this section is to explain how to use long-range technologies for teaching IoT communication at undergraduate Computer Engineering courses. Effectively, a LoRaWAN can be deployed in a university area, however there are some limitations, as follows:

- Data size for sending and receiving to/from end-nodes: these networks send only small data chunks at regular periods. Thus, the development of novel applications must consider this limitation.
- Performance: these networks are very slow compared to conventional Wi-Fi, which operates at 2.4 GHz or 5 GHz. This characteristic restricts real-time applications.
- Very low power consumption: the whole infrastructure consumes little power resources to be active. This feature is useful for passive applications that should not be constantly powered, e.g., applications for measuring temperature, humidity, and atmospheric pressure.

The infrastructure allows the wireless connection of low-cost IoT end devices. Figure 9.4 shows this logical network topology.

The first step was to set up a single compatible antenna at the top of the university building. The expected coverage area was empirically measured and reached over 5 km in the urban area. The frequency band is different from the conventional 2.4 GHz of Wi-Fi access points, so no interference was perceived within the campus. It was recommended to the students to use LoRa1276 modules in their IoT devices with a frequency of 915 MHz to connect with the antenna and avoid interference with other frequencies. The gateway was configured behind the same Internet firewall of the campus, and it was able to guarantee minimal security from outside traffic.

Figure 9.5 shows the estimated coverage area with a single antenna. This much area is useful to allow many IoT connections in the outside area. We believe that this feature is very useful to allow experiments at large distances without requiring the hardware apparatus to be put directly in contact with the gateway. Other conventional Wi-Fi technologies are very limited in this aspect.

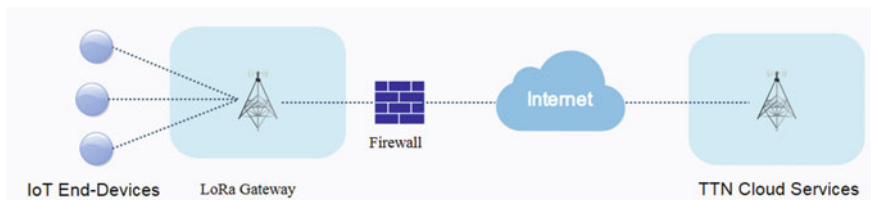
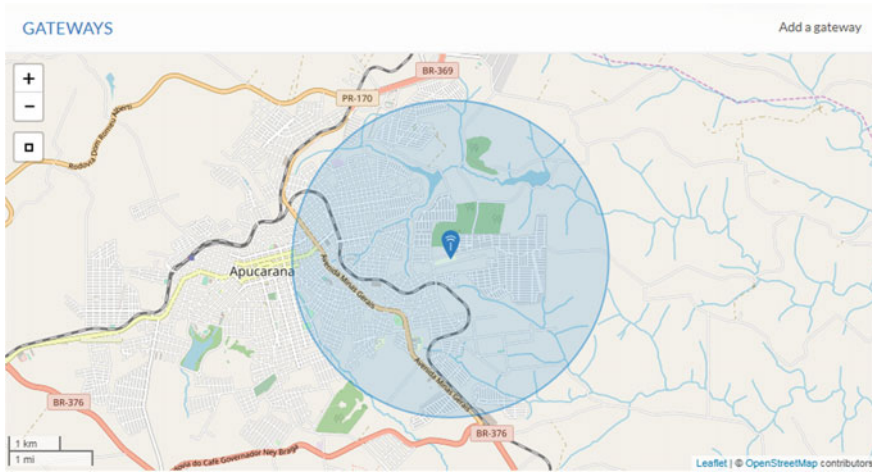


Fig. 9.4 Logical topology of LoRaWAN in UTFPR Campus Apucarana



**Fig. 9.5** LoRaWAN coverage area in UTFPR Campus Apucarana

### 9.4.1 Specification of Components

The establishment of this infrastructure depends on many components. This section describes the IoT components used to establish communication between the end-nodes and the IoT cloud network.

- LoRait: it is an MTAC-915 from MultiTech [39]. It is a concentrator module connected to raspberry PI version 3 through a Mini Pci-E M2 socket/USB board. The MTAC-915 is also connected to an ASA-920 antenna through a 40-cm 50- $\Omega$  RF cable.
- RF LoRa 915 MHz V2.0 IoT module: it works as a transmitter and receiver, but not both at same time (it is not full-duplex). Modulation modes available are OOK, FSK, and LoRa. Error detection is performed with FEC and checksum. This module uses only the lower layers of the OSI model (it is possible to use an existent protocol or a new one). Regarding the data transmission interval, data packets are sent at predefined periods, not continuously.
- NodeMCU dev 0.9 (or more recent): these devices are able to send/receive messages through the antenna without high packet losses. We performed tests with Arduino, but its low memory capacity to process networks is not adequate to use with the RF LoRa1276 module.
- ASA-920 gateway antenna: this operates at 915 MHz; its specifications are shown in Table 9.1.

**Table 9.1** LoRaWAN antenna specifications

Frequency	902/928 MHz
Model	ASA-920
Polarization	Vertical
Nominal impedance	50 Ω
Maximum potency	100 W
Gain	8.15 dBi
Diameter	16.44 mm
Total length	385 mm
Weight	230 g

### 9.4.2 LoRaWAN Infrastructure

This section describes the infrastructure used to establish communication using the LoRa gateway with a set of IoT end devices. This LoRaWAN infrastructure uses a gateway to forward packets from devices to an application server. Next, we explain our methodology to create this LoRaWAN infrastructure.

Our LoRa gateway runs the Raspbian operating system, and some steps were adapted from [40] to configure the MTAC-915 hardware. For the gateway, we used additional libraries to support SPI/I2C control via FTDI chips. Raspbian needs these libraries to operate MTAC-915 through the Mini Pci-E M2 socket/USB hardware board. This Mini Pci-E M2 socket/USB board should be recognized as an FT232H USB-to-UART. Therefore, the following software need to be installed:

- libftdi-dev, from the debian package management software;
- <https://github.com/devtys0/libmpsse>, using git software.

Compiling libmpsse (`./configure--prefix=/usr && make && make install`) installs the following files: `/usr/lib/libmpsse.so`, `/usr/lib/libmpsse.a`, and `/usr/include/mpsse.h`. In order to recognize the Mini Pci-E M2 socket/USB hardware board as an FT232H USB-to-UART, an additional rule file must be downloaded from [41] and inserted into the `/etc./udev/rules.d` directory. In sequence, the following commands need to be executed:

- `sudo udevadm control--reload-rules && sudo udevadm trigger && sudo adduser pi plugdev`
- If all these steps are executed correctly, the “lsusb” command should output something like this: `Bus 001 Device 003: ID 0403:6014 Future Technology Devices International, Ltd FT232H Single HS USB-UART/FIFO IC.`

The next step refers to the LoRa packet forwarder. Building a gateway with Raspberry PI generally uses the Semtech packet forwarder [42], which employs UDP to forward uplink messages from nodes to the network servers. We chose the poly-packet forwarder version from [43], which improves the Semtech packet forwarder with the TTN gateway connector [44]. Moreover, it can forward packets to up to four

```

$INSTALL_DIR/dev/lora_gateway/libloragw
#sed -i -e 's/PLATFORM= .*/PLATFORM= imst_rpi/g' library.cfg
#sed -i -e 's/CFG_SPI= .*/CFG_SPI= native/g' library.cfg
#sed -i -e 's/DEBUG_GPS= .*/DEBUG_GPS= 1/g' library.cfg
sed -i -e 's/PLATFORM= .*/PLATFORM= multitech/g' library.cfg
sed -i -e 's/CFG_SPI= .*/CFG_SPI= ftdi/g' library.cfg
make

```

**Listing 9.1** Addition to build-pi.sh script

different LoRa Servers, enabling tests with private Lora Servers. Using the repository from [43], the code as shown in Listing 9.1 was added between original lines 72 and 73 in the build-pi.sh script to enable support for MTAC-915 through USB-UART.

Also, it is necessary to install libusb support:

- `sudo apt install libusb-1.0-0-dev && sudo apt install libusb-1.0-0 && sudo apt install libusb-dev`
- `sudo build-pi.sh`.

The latter will install the necessary source code in `/opt/ttn-gateway/dev` and the packet forwarder binary in `/opt/ttn-gateway/mp_pkt_fwd`.

Finally, to use the TTN cloud service, it is necessary to choose the correct file configuration from [44], according to the regional parameters, saving it as `global_conf.json` in the `/opt/ttn-gateway` folder. In our case, we use the `AU-global_conf.json` as the `global_conf.json` file because it is the same frequency plan for Brazil. However, we must change the following parameter:

- “`clksrc`”: 1 to “`clksrc`”: 0 because of the MTAC hardware.
- Recently, the code as shown in Listing 9.2 was added to all `global_conf.json` from [44] between lines 4 and 5.

The last modification is to add the configuration, as shown in Listing 9.3, to the `/opt/ttn-gateway/local_conf.json` script, which is based on `local_conf.json` from [43]. Example of a second Lora Server for a poly-packet feature with a simple Semtech server type schema is also presented.

There are many possibilities to run `mp_pkt_fwd` during the raspberry PI boot. We chose `/etc/rc.local` with the following commands: `cd /opt/ttn-gateway&& ./mp_pkt_fwd -l output.txt &`.

For our case study, we use nodeMCU as an IoT end device to establish a wireless connection with the LoRa antenna. The communication between the host and the LoRa module is done with the serial peripheral interface (SPI) protocol. The connections are informed in Table 9.2.

```

"clksrc": 1,
"clksrc_desc": "radio_1 provides clock to concentrator for most
devices except MultiTech. For MultiTech set to 0.",

```

**Listing 9.2** Addition to the `global_conf.json` script

```

{
  /* Put there parameters that are different for each gateway (eg.
  pointing one gateway to a test server while the others stay in pro-
  duction) */
  /* Settings defined in global_conf will be overwritten by those in
  local_conf */
  "gateway_conf": {
    "gateway_ID": "HEX NUMBER FROM THE MTAC HARDWARE", /* you must pick
    a unique 64b number for each gateway (represented by an hex string) */
    "gps": true,
    "beacon": false,
    "monitor": false,
    /* Systems (set logger to true for logs per (!) packet) */
    "logger": true,
    /* Streams */
    "upstream": true,
    "downstream": true,
    "ghoststream": false,
    "radiostream": true,
    "statusstream": true,
    /* node server, (for standard server, fall back for poly packet
    &multi protocol packet server) */
    "server_address": "127.0.0.1",
    "serv_port_up": 1680,
    "serv_port_down": 1681,
    /* node servers for poly packet server (max 4 enabled, rest is ig-
    nored) */
    "servers": [
      {
        "serv_type": "ttn",
        "server_address": "A SERVER ADDRESS CHOSEN FROM TTN CONSOLE:1883",
        "serv_gw_id": "GATEWAY ID FROM TTN CONSOLE",
        "serv_gw_key": "KEY GENERATED FROM TTN CONSOLE",
        "serv_enabled": true
      },
      {
        "serv_type": "semtech",
        "server_address": "PRIVATE SEMTECH LORA SERVER IP ADDRESS",
        "serv_port_up": 1700,
        "serv_port_down": 1700,
        "serv_enabled": true
      }
    ],
    /* adjust the following parameters for your network */
    "keepalive_interval": 10,
    "stat_interval": 30,
    "push_timeout_ms": 100,
    /* forward only valid packets */
    "forward_crc_valid": true,
    "forward_crc_error": false,
    "forward_crc_disabled": false,

```

**Listing 9.3** Configuration added to the /opt/ttn-gateway/local\_conf.json script

```

/* GPS configuration */
"gps_tty_path": "/dev/ttyAMA0",
"fake_gps": true,
"ref_latitude": YOUR LATITUDE HERE, /* put your latitude here */
"ref_longitude": YOUR LONGITUDE HERE, /* put your longitude here */
"ref_altitude": YOUR ALTITUDE HERE,
/* Ghost configuration (for simulating nodes) */
"ghost_address": "127.0.0.1",
"ghost_port": 1918,
/* Monitor configuration (for remote access through the fire-
wall/nat) */
"monitor_address": "127.0.0.1",
"monitor_port": 2008,
"ssh_path": "/usr/bin/ssh",
"ssh_port": 22,
"http_port": 80,
"ngrok_path": "/usr/bin/ngrok",
"system_calls": ["df -m", "free -h", "uptime", "who -a", "uname -a"],
/* Performance updates (if empty, nothing is send/written) */
"stat_format": "semtech", /* semtech or idee_verbose or
idee_concise. */
"stat_damping": 50, /* 1 for least damping up to 99 for most damp-
ing. */
"stat_file": "stats.txt", /* Put or the whole path, or only a file
name */
/* For human communication */
"platform": "*", /* Platform definition, put a asterix here for
the system value, max 24 chars. */
"contact_email" : "EMAIL CONTACT HERE", /* Email of gateway opera-
tor, max 40 chars*/
"description": "SIMPLE DESCRITPION HERE" /* Public description of
this device, max 64 chars */
}
}

```

**Listing 9.3** (continued)

### 9.4.3 Registration of IoT End-Devices in TTN

In this section, we explain how to register IoT end-devices for using the LoRaWAN in TTN. This registration is necessary to identify uniquely the end devices that are in the same pool of communication: TTN OTAA over-the-air activation (OTAA).

- In the Arduino IDE, the following libraries are used: ESP8266, from the ESP8266 community, and the MCCI Arduino LoRaWan Library forked from the IBM LMIC library and available in the Arduino Libraries Management. The MCCI Arduino LoraWan Library needs a setup with the following values in the `lmic_project_config.h` file from the `lmic_library_master/library` folder, as shown in Listing 9.4.
- Create an account on <https://thethingsnetwork.org>.



**Table 9.2** Links between LoRa1276 and NodeMCU modules

LoRa1276 module	NodeMCU dev0.9
Pin/function	Pin/function
1/GND	GND/GND
2/NC	Unused
3/NC	Unused
4/SCK	D5/GPIO14
5/MISO	D6/GPIO12
6/MOSI	D7/GPIO13
7/NSS	D8/GPIO15
8/DIO2	Unused
9/DIO1	D2/GPIO4
10/DIO0	D1/GPIO5
11/VCC	3.3 V
12/RESET	D0/GPIO16

```
#define CFG_au921 1
#define CFG_sx1276_radio 1
#define LMIC_DEBUG_LEVEL 1
```

**Listing 9.4** Definition of the frequency band for NodeMCU

- The next step is to register a new IoT application in the TTN cloud service. In the Things Network Console, register a new Application as shown in Fig. 9.6. The required fields are Application ID (e.g.: a54545454) and the regional Handler Registration (e.g., ttn-handler-brazil).
- Next, we need to register our devices as in Fig. 9.7. The Device ID is set uniquely, e.g., a54545454\_nicerf-1. The device EUI is generated automatically by the network server. Also, the App Key should be unique for each device, so this unique key is automatically generated by the cloud service. The App Key is an AES-218 bit used for symmetric encryption based on the Rijndael cipher, a popular symmetric encryption algorithm. It offers nine combinations of key and block length by using variable key lengths of 128, 192, or 256 bits key to encrypt data blocks that are 128, 192, or 256 bits long [6].
- In the device overview, we click on the hex/C-style icon, then on the double arrows icon to change the Device EUI to hexadecimal, and its representation to LSB. The same applies to the Application EUI, i.e., LSB. We also click on the hex/C-style icon in the App Key to display the hexadecimal values. For this case only, we use the MSB representation, as shown in Fig. 9.8.
- In the Arduino IDE, we create a starter code from this Arduino example for TTN with the Device EUI, Application EUI, and App Key information. We keep the Arduino serial monitor open with 115,200 baud/rate during the deployment of our code to observe the messages of establishing a connection with the LoRaWAN gateway. We set the Arduino board of the NodeMCU 0.9 ESP12 module with

Applications > Add Application

### ADD APPLICATION

**Application ID**  
The unique identifier of your application on the network

a123456789

**Description**  
A human readable description of your new app

NodeMCU\_tutorial

**Application EUI**  
An application EUI will be issued for The Things Network block for convenience, you can add your own in the application settings page.

EUI issued by The Things Network

**Handler registration**  
Select the handler you want to register this application to

ttn-handler-brazil

Cancel Add application

Fig. 9.6 Adding a new application in the TTN cloud server

Applications > a123456789 > Devices

### REGISTER DEVICE

**Device ID**  
This is the unique identifier for the device in this app. The device ID will be immutable.

a123456789\_nicerf-1

**Device EUI**  
The device EUI is the unique identifier for this device on the network. You can change the EUI later.

x 0 bytes

Device EUI must consist of exactly 8 bytes

**App Key**  
The App Key will be used to secure the communication between you device and the network.

this field will be generated

**App EUI**

Cancel Register

Fig. 9.7 Registering a new node in the TTN

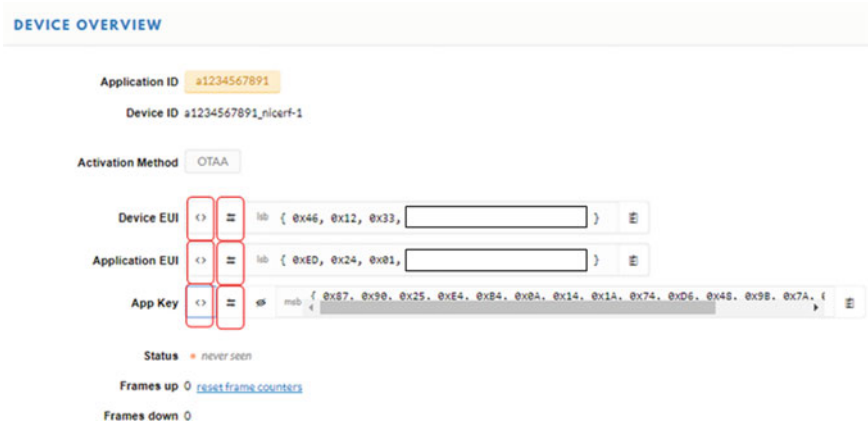


Fig. 9.8 Acquiring of LSB/MSB hexadecimal values

a flash size of 4M (3M SPIFFS). Figure 9.9 illustrates the messages during the joining event (EV\_JOINING). After this step, the end-node can send/receive data to/from the TTN cloud server.

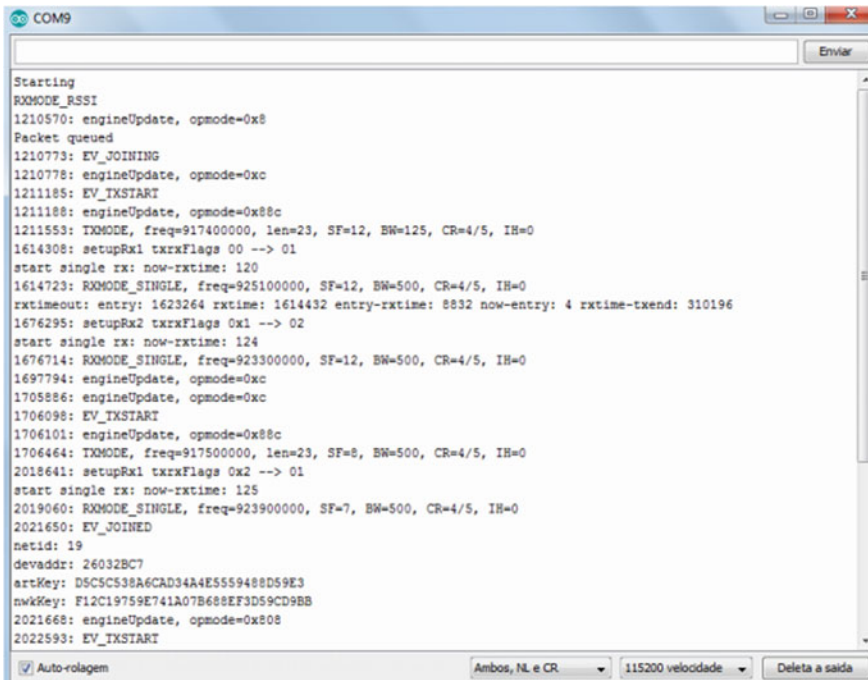


Fig. 9.9 EV\_JOINING data messages

To enter a TTN network, each end device needs to be personalized and activated [45]. The activation may be achieved by over-the-air-activation (OTAA) or activation-by-personalization (ABP). In the OTAA procedure, end devices transmit a *join\_request* to the network server (NS), which validates them and replies with a *join\_accept* message. In the ABP procedure, the manufacturers put the session keys on the end devices from a predefined pool of keys, or the application manager creates such keys and distributes them manually. In our scenarios, the OTAA procedure was used to establish communication between end devices and the gateway.

The EV\_JOINING (*join\_request* message) is necessary to guarantee minimal security through the authentication process. The information on keys is setup inside the Arduino application. EV\_JOINING verifies if the AppKey is correct and if it is registered for this end-node device. This symmetric key should be unique for each end device. Thus, if a key is compromised, a single end node over the entire network will be affected. OTAA uses *join-request* and *join-accept* messages to validate keys [6].

## 9.5 Experimental Evaluation

Our methodology included the evaluation of several experiments as part of a regular undergraduate computer engineering course. The students were invited to design and develop possible IoT applications for smart cities using the LoRa infrastructure available at the university campus. These experiments were running all at the same time and using the same infrastructure for different purposes. Prototypes for possible commercial applications using either Arduino boards or ESP8266 modules were developed and interfaced to the LoRa gateway via HopeRF RFM95W. We highlight that these experiments did not interfere with the existing wireless communication or other regular measuring sensors. The next subsections present such experiments.

### 9.5.1 Smart Trash Can System

In this subsection, a smart trash can system is presented. Figure 9.10 shows the prototype for measuring the trash level via an ultrasonic sensor. When the trash can is full, the microcontroller sends an e-mail to the trash owner. This kind of application has the potential to be used in a smart city for monitoring empty/full trash cans and optimizing the garbage collector. For example, urban areas where trash cans are constantly full should be prioritized. Furthermore, this simple application could be used as an indicator of the best time of day to run trash collection over the entire city. Another aspect regards the possibility of redistributing the trash cans over the areas with more disposals and evaluating the kind of disposals by local area and time of day.



**Fig. 9.10** Smart trash can

### ***9.5.2 Wind Speed Meter System***

In this subsection, we present a wind speed meter system, the prototype of which is shown in Fig. 9.11. This system uses an anemometer and a microcontroller which counts the number of rotations per minute to measure wind speed. The results are sent to the LoRa server and made available to the final user via a Web page. This prototype has the possibility of being commercially applied in coastal areas to indicate, via smartphones, the best times for navigation or even to inform tourists about the local weather conditions. Another application is for rural areas, as a sensor for measuring local weather changes for spraying herbicides over the crops with planes.

### ***9.5.3 Weather Station System***

In this subsection, we present a weather station system developed by the students. This prototype, shown in Fig. 9.12, uses a scale rain gauge to measure the amount



**Fig. 9.11** Wind speed meter



**Fig. 9.12** Small weather station

of rain, besides providing data such as temperature and humidity. Small weather stations are relatively simple, but their applicability in vulnerable areas may be very important. For example, Brazilian areas where the incidence of rain exceeds the regular volume predicted for the same period could potentially indicate a risk of floods. This indicator could send an alert through many media (sonorous, SMS, luminous, etc.) to the area residents.

### 9.5.4 *Smart Greenhouse System*

Here, we present a smart greenhouse (Fig. 9.13) which provides scheduled watering times, also providing to the final user, via a Web page, the temperature and humidity of both the soil and the air. A large number of rural applications could be leveraged from this prototype, such as organic planting and animal breeding. Many of these applications are already carried out with human intervention in regular periods to empirically evaluate the need for increasing/decreasing the power supply for spreading water, wind, and other supplies. Another consideration is the inherent LoRaWAN feature of establishing communication at large distances. Especially in rural areas,



**Fig. 9.13** Smart greenhouse

this feature may potentially reduce the risks of faults with simple measuring by smart devices, which send/receive information about the status of its property owner. For example, a short outage could be informed to the administrator, signaling that an intervention is necessary.

### **9.5.5 Feeder System**

Lastly, a smart dog feeder system was developed by students and is depicted in Fig. 9.14. This equipment releases the feed gate at user-defined times. A potential application is for domestic animal feeding. This sample could be extended to locate the dog with a collar in urban areas and open public feeding gates for any animal correctly identified.

### **9.5.6 Discussion**

By encouraging students to build up creativity by developing IoT products, it is expected that it is possible to prepare a new generation of engineers who will be prepared to handle the connectivity that will be required in the industry. These prototypes were developed with low-cost products and LoRaWAN. Although these experiments are very limited for large-scale usage, they showed some important aspects, as follows, that motivate further studies:

- Low consumption powered by very long-life batteries;
- Network devices that communicate with low frequency and reduced amount of network data;
- Low data transfer;
- Large wireless coverage ranges from 1 km in urban areas to 10 km in open areas. In this sense, it is possible to send small amounts of data at larger distances than with other wireless technologies;
- Minimal wireless interference and reduced shortage when widening the data network;
- Easy experimental evaluation of new applications without compromising the current wireless communication.

## **9.6 Conclusion**

Many enterprises evaluate the possibility of using long-range transmission in new applications where conventional wireless communications are not feasible. LoRa technologies are suitable for non-critical applications where small chunks of data are



**Fig. 9.14** Smart dog feeder



sent periodically and may service a very large number of IoT end devices for long periods. Although it may be difficult to predict the success cases, many academics have contributed to leverage potential applications in collaboration with the industry. The main advantage in academia is the possibility of evaluating many new potential research efforts with low costs and without compromising applications.

In a sense, long-range technologies are relatively new but have a high potential for being in the industry. A vision of a global wide LPWAN is seen as a 2.4-GHz ISM by RPMA [7], instead of regional spectrum unlicensed Sigfox/LoRa technologies. However, for covering areas up to 10 km, non-critical short length data are sufficient to service many applications where conventional wireless is not feasible. According to [7], the 2.4-GHz band uses 80 MHz, and this large portion of the frequency spectrum is favorable to high coverage. The authors also state that a capacity to support end devices is preferable for the coverage area. A recent study points out that, to send short messages of up to 32 bytes in real-world conditions, an RPMA access point can receive more than 500,000 messages/hour against 2000 messages/hour with a LoRa base station. These considerations are important for enterprises that need to provide services for a large number of IoT devices for long periods, or even for smart city applications.

However, some challenges are still unsolved. Ingenu [7] states that LoRa Sig-Fox technologies, although well-known in the market, do not allow connections for a sufficient number of endpoints to make long-term economic sense. Ingenu also affirms that additional network infrastructure cannot be added once the capacity has been exhausted. Related to similar technologies, such as random phase multiple access (RPMA) [7], LoRa support much fewer endpoints for a given network. Another aspect mentioned is that LoRa is not complementary to cellular LPWA, and therefore constrained to fit their hardware into existing platforms. Besides, the mesh topology used by such networks is not power-efficient and may reduce the performance and quality of the services. Many LoRa devices are less expensive and more accessible than RPMA solutions. Navarro et al. [25] affirm that LPWAN technologies have much lower cost compared to cellular networks. Other consideration mentioned in [46] is about LoRa antenna interferences. The authors argue that current LoRa deployments use default static setups that could lead to inter-network interference. So, it is recommended to use mechanisms for dealing with this interference ahead of the simple installation of a new gateway [47].

In this book chapter, we have described long-range technologies based on the most recent literature reviews. Our focus was the evaluation of how a LoRaWAN infrastructure may be deployed in academia before effectively being used in industrial sectors.

**Acknowledgements** The authors gratefully acknowledge the contribution of the Brazilian Computer Systems Research Group ([dgp.cnpq.br/dgp/espelhogrupo/3644261646894579](http://dgp.cnpq.br/dgp/espelhogrupo/3644261646894579)). The authors also thank the collaboration of students from the Programming Fundamentals discipline of the Computing Engineering course of the Apucarana campus of the UTFPR.

## References

1. Ankrah S, AL-Tabbaa O (2015) Universities–industry collaboration: a systematic review. *Scandinavian J Manag* 31(3):387–408
2. Instructables (2018) Arduino Internet de Las Cosas: Usando NICERF LoRa1276, Sept 2018. Available at: <https://www.instructables.com/id/Arduino-Internet-De-Las-Cosas-Usando-NiceRf-LoRa12>
3. De Oliveira LR (2018) Setup LoRa com Arduino, Raspberry Pi e shield Dragino. Available at: <https://www.embarcados.com.br/lora-arduino-raspberry-pi-shield-dragino/>. Access in Oct 2018
4. Gemalto.com (2018) What is low power wide area network (LPWAN) technology? Available at: <https://www.gemalto.com/m2m/development/innovation-technology/low-power-wide-area-technology>
5. Hoperf Electronics (2018) Introduction LoRa & module RFM95, Oct 2018. Available at: [https://www.youtube.com/watch?time\\_continue=67&v=zWPPfzEpmfs](https://www.youtube.com/watch?time_continue=67&v=zWPPfzEpmfs)
6. Cisco Cybersecurity (2018) Cybersecurity operations course. Available at: <https://1400514.netacad.com/courses/736908/modules/items/51792465>
7. Ingenu.com (2018) How RPMA works—the making of RPMA, e-book. Available at: <https://www.ingenu.com/portfolio/how-rpma-works-the-making-of-rpma/>
8. LoRa Alliance (2018) LoRaWAN 1.1 specification, Sept 2018. Available at: <https://loralliance.org/resource-hub/lorawantm-specification-v11>
9. Thing Forward (2018) Getting started with LoraWAN, the things network and platform IO, Oct 2018. Available at: <https://www.thingforward.io/techblog/2017-09-27-getting-started-with-lorawan-thethingsnetwork-and-platformio.html>
10. Laurenson T (2018) Dragino LoRa shield node configuration for AU915 (updated), Oct 2018. Available at: <https://www.thomaslaurenson.com/blog/2018/07/21/dragino-lorashield-on-AU915-using-arduino-lmic-library/>
11. da Silva Neto E (2018) Gateway LoRa: soluções open source hardware. <https://www.embarcados.com.br/gateways-lora-open-source-hardware/>. Dez 2018
12. Haxhibeqiri J, Karaağaç A, Van den Abeele F, Joseph W, Moerman I, Hoebeke J (2017) LoRa indoor coverage and performance in an industrial environment: case study. In: IEEE ETFA2017, the 22nd IEEE international conference on emerging technologies and factory automation, pp 1–8
13. Yi S, Chun S, Lee Y, Park S, Jung, S (2013) Machine type communication (MTC). In: *Radio protocols for LTE and LTE-advanced*. Wiley
14. Anteur M, Deslandes V, Thomas N, Beylot A (2015) Ultra narrow band technique for low power wide area communications. In: 2015 IEEE global communications conference (GLOBECOM), San Diego, CA, pp 1–6 (2015)
15. Raza U, Kulkarni P, Sooriyabandara M (2017) Low power wide area networks: an overview. *IEEE Commun Surv Tutor* 19(2), 855–873
16. Do M, Goursaud C, Gorce J (2014) Interference modelling and analysis of random FDMA schemes in ultra narrowband networks. In: AICT2014: the tenth advanced international conference on telecommunications
17. Zhang K, Marchiori A (2017) Crowdsourcing low-power wide-area IoT networks. In: 2017 IEEE international conference on pervasive computing and communications (PerCom), Kona, HI, pp 41–49
18. LoRaWAN Backend Interfaces. <https://loralliance.org/sites/default/files/2018-04/lorawantm-backend-interfaces-v1.0.pdf>
19. LoRa Alliance (2018) What is LoRa alliance? Available at: <https://loralliance.org/about-lora-alliance>
20. Gerber A (2018) Criando cidades conectadas com tecnologias de IoT novas e existentes. Available at: <https://www.ibm.com/developerworks/br/library/iot-1p201-iot-connected-cities/index.html>

21. Semtech.com (2018) What is LoRaWAN?. Available at: <https://www.semtech.com/lora/what-is-lora>
22. Actility.com (2018) LoRa device developer guide, Sept 2018. Available at: <https://www.actility.com/resources/documentation/>
23. Microchip.com (2018) Embedded wireless: low-power wide-area network. Available at: <https://www.microchip.com/design-centers/wireless-connectivity/low-power-wide-area-networks/lora-technology>
24. Cisco.com (2018) Cisco wireless gateway for LoRaWAN data sheet. Available at: <https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-737307.html>
25. Navarro-Ortiz J, Sendra S, Ameigeiras P, Lopez-Soler JM (2018) Integration of LoRaWAN. *IEEE Commun Mag* 56(2):60–67
26. LoRa Alliance (2018) LoRaWAN 1.1 regional parameters. Available at: [https://lora-alliance.org/sites/default/files/2018-04/lorawantm\\_regional\\_parameters\\_v1.1rb\\_-\\_final.pdf](https://lora-alliance.org/sites/default/files/2018-04/lorawantm_regional_parameters_v1.1rb_-_final.pdf), Dec 2018.47. LoRa Alliance (2018)
27. Anatel (2018) Agência Nacional de Telecomunicações. Ato no. 14448, de 04 de Dezembro de 2017. Requisitos Técnicos para a Avaliação da Conformidade de Equipamentos de Radiocomunicação de radiação restrita. Available at: [https://sei.anatel.gov.br/sei/publicacoes/controlador\\_publicacoes.php?acao=publicacao\\_visualizar&id\\_documento=2549681&id\\_orgao\\_publicacao=0](https://sei.anatel.gov.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_documento=2549681&id_orgao_publicacao=0)
28. Hoeller A, Souza RD, Alcaraz López OL, Alves H, de Noronha Neto M, Brante G (2018) Analysis and performance optimization of LoRa networks with time and antenna diversity. *IEEE Access* 6:32820–32829
29. Catherwood PA, McComb S, Little M, McLaughlin JAD (2017) Channel characterisation for wearable LoRaWAN monitors. In: Loughborough antennas & propagation conference, Loughborough, pp 1–4
30. Croce D, Gucciardo M, Mangione S, Santaromita G, Tinnirello I (2018) Impact of LoRa imperfect orthogonality: analysis of link-level performance. *IEEE Commun Lett* 22(4):796–799
31. Lavric A, Popa V (2017) Internet of things and LoRa™ low-power wide-area networks challenges. In: 2017 9th international conference on electronics, computers and artificial intelligence (ECAI), Targoviste, pp 1–4
32. Ferreira DVM, Coelho VN, Silva SM (2017) Plataforma open-hardware de baixo custo para teste de dispositivos IoT voltados para smart cities. Anais do I workshop of computational intelligence and smart cities (WCISC 2017). Available at: <https://creating.city/wcisc2017/proceedings-wcisc2017.pdf>
33. Petäjäjärvi J, Mikhaylov K, Hämäläinen M, Iinatti J (2016) Evaluation of LoRa LPWAN technology for remote health and wellbeing monitoring. In: 2016 10th international symposium on medical information and communication technology (ISMICT), pp 1–5
34. Varsier N, Schwoerer J (2017) Capacity limits of LoRaWAN technology for smart metering applications. In: 2017 IEEE international conference on communications (ICC), pp 1–6
35. Wang S, Zou J, Chen Y, Hsu C, Cheng Y, Chang C (2018) Long-term performance studies of a LoRaWAN-based PM2.5 application on campus. In: 2018 IEEE 87th vehicular technology conference (VTC Spring), Porto, pp 1–5
36. Wan X, Yang Y, Cui J, Sardar MS (2017) Lora propagation testing in soil for wireless underground sensor networks. In: 2017 Sixth Asia-Pacific conference on antennas and propagation (APCAP), Xi'an, pp 1–3
37. Ducrot N, Ray D, Saadani A et al (2018) Lora device developer guide. Available at: <https://www.actility.com/wp-content/uploads/2016/12/LoRa-Device-Developer-Guide-Orange.pdf>
38. Amazon Web Services (2018) O que Internet da Coisas, Sept 2018. Available at: <http://aws.amazon.com/pt/iot/>
39. Multitech.com (2018) IoT gateways, routers, and modems. Available at: <https://www.multitech.com/products/gateways-routers-modems>
40. Ayuso N (2018) Lora gateway project. [https://github.com/mirakonta/lora\\_gateway/wiki](https://github.com/mirakonta/lora_gateway/wiki)
41. Ayuso N (2018) 99-libftdi.rules. [https://raw.githubusercontent.com/mirakonta/lora\\_gateway/master/libloragw/99-libftdi.rules](https://raw.githubusercontent.com/mirakonta/lora_gateway/master/libloragw/99-libftdi.rules)

42. Coracin M (2018) Packet forwarder. [https://github.com/Lora-net/packet\\_forwarder](https://github.com/Lora-net/packet_forwarder)
43. Kersing J (2018) Multi protocol packet forwarder supporting the TTN gateway-connector protocol. [https://github.com/kersing/packet\\_forwarder](https://github.com/kersing/packet_forwarder)
44. Visser H (2018) Embedded C library for the things gateway and Linux-based gateways to connect to the things network. <https://github.com/TheThingsNetwork/ttn-gateway-connector>
45. Butun I, Pereira N, Gidlund M (2018) Analysis of LoRaWAN v1.1 security: research paper. In: Proceedings of the 4th ACM MobiHoc workshop on experiences with the design and implementation of smart objects (SMARTOBJECTS '18). ACM, New York, NY, USA, Article 5, 6 pages. <https://doi.org/10.1145/3213299.3213304>
46. Voigt T, Bor M, Roedig U, Alonso J (2017) Mitigating inter-network interference in LoRa networks. In: Proceedings of the 2017 international conference on embedded wireless systems and networks (EWSN '17). Junction Publishing, USA, 323–328.37
47. Adelantado F, Vilajosana X, Tuset-Peiro P, Martinez B, Melià-Seguí J, Watteyne T (2017) Understanding the limits of LoRaWAN. IEEE Commun Mag

**Part IV**  
**Applications and Use Case Scenarios**

# Chapter 10

## Implementation of Industrial Internet of Things in the Renewable Energy Sector



Somudeep Bhattacharjee and Champa Nandi

**Abstract** A smart microgrid is becoming a popular approach for power generation due to the scarcity of fossil fuel, increasing air pollution, increasing demand for cleaner energy resources, and better energy utilization. Presently, sensor technology, big data, and data analytics are the hot topics for research for optimizing business operations, such as efficient and balancing supply versus demand as customers connect to a smart microgrid. These advancements based on smart devices and their connectivity via the Internet have given rise to what is now being known as Industrial Internet of things (i.e., industrial IoT or IIoT). These devices help to maximize operational efficiency, optimize business operation, and protect the system. This chapter presents detailed discussion of the concept of IIoT, history and applications of IoT, developments in the energy sector, introduction to renewable energy, role of IoT in developing smart grids and smart microgrids, role of IIoT to combat the challenges of renewable energy sector, and the future vision of the IIoT paradigm in the energy industry. The main objective is to study and analyze the IIoT-based renewable energy sector for reducing fossil fuel usage, increasing cleaner energy resources usage, and better energy utilization. It is also suggested that the IIoT-based energy systems can easily tackle the problems of non-availability of individual renewable energy sources by monitoring energy usage, energy generation, and its integration with other sources.

**Keywords** Industrial Internet of Things · IIoT · Energy management · Renewable energy · Smart grid · Smart microgrid · Distributed energy · I4.0

### 10.1 Introduction

Increasing demand for electric power, using coal for electricity generation, increase in population, and the utilization of renewable energy are the fundamental reasons behind the changes coming to the electricity sector. Currently, 85% of the world population utilizes electricity and 40% of world electricity originates from coal. For

---

S. Bhattacharjee · C. Nandi (✉)  
Department of Electrical Engineering, Tripura University, Suryamaninagar 799022, India  
e-mail: [cnandi@tripurauniv.in](mailto:cnandi@tripurauniv.in)

© Springer Nature Switzerland AG 2019  
Z. Mahmood (ed.), *The Internet of Things in the Industrial Sector*, Computer Communications and Networks, [https://doi.org/10.1007/978-3-030-24892-5\\_10](https://doi.org/10.1007/978-3-030-24892-5_10)

electricity generation, coal produces 70% of the carbon dioxide (CO<sub>2</sub>) emissions that are proving to be destructive to the environment and human health. To reduce the current levels of emissions, the need for renewable energy is rising. Sustainable sources (such as biomass, hydropower, geothermal, wind, and solar) are becoming popular and in high demand. Battery technology is also becoming an attractive option [1].

Because of the shortage of fossil fuel and increasing pollution, the destiny of technology upgrade and further research relies upon the use of cleaner energy production sources and better use of the available energy. So, to accomplish this objective, government and utility agencies are aiming to develop new energy infrastructures known as the “smart grids” and “smart microgrids”. The reason for the smart grids is to adequately deal with the processes of energy transmission, generation, and distribution. Everyone of the stakeholders, including the distributors, consumers, and producers, is permitted to have a two-path communication to create, consume, and distribute energy in an effective way. The greatest energy consumers are buildings, for example, houses, structures, and workplaces in developed countries. The consumption rate is considerably higher in the undeveloped countries because of the absence of adequate industrial sector, in some cases. Hence, energy efficiency can be accomplished by proficiently utilizing the accessible energy sources. The target can be fulfilled if the energy use can be accurately determined in real time. This data must be transmitted to the local smart grid to accomplish the objective of energy minimization. Moreover, the energy utilization can be monitored if the heavy-duty gadgets are planned in a robotized and productive way. Another alternative is to utilize the renewable sources, for example, solar cells and wind turbines that lessen the reliance on the power supply from energy organizations. In addition, energy protection and efficient storage are the most vital in fuel energy production.

The issue of anticipating and reacting to the variable energy demand turns out to be very difficult because of the expansion of renewable energy sources, for example, wind and sun. The energy production planning is required to optimize the energy use and its cost. The planning framework needs to think about various energy resources available and then carry out the optimization based on feedback from various related aspects. The priorities and constraints of consumers should be looked at by the self-managing energy system (SES) for the optimization of energy use by utilizing this data, alongside the demand for power and supply forecast. The SES should have the capacity to incorporate renewable energy, for example, solar and wind energy, in the framework [2–4].

The energy utilization requirements are communicated to the framework by means of the Internet of things (IoT) [2] that helps to communicate with various IoT-based devices and gives feedback to microgrids to carry out the optimizing choice. Four targets can be accomplished utilizing the proposed design as follows [2]:

- First, it designs a localized Internet of things, for transmitting and getting data to/from smart devices and consumers.
- Second, it controls the energy consumption of devices, utilizing the priorities and constraints set by the buyers.



- Third, it gives feedback to the customers of their energy utilization pattern, so as to save energy and cost.
- Fourth, it incorporates renewable sources of energy into the network.

For controlling, overseeing, and accomplishing the two-sided communication with latest advancements in the energy sector, IIoT plays a critical role, particularly with respect to renewable energy technologies. The Internet of things (IoT) is an umbrella vision that has Industrial Internet of things (IIoT) as a particular case. It is a network of smart devices and things that generates gigantic amount of data that is then sent to central cloud-based services where it is processed and further transmitted [5]. Currently, sensor technology, big data, and analytics are receiving more concentration so as to optimize tasks, for example, proficiently adjusting demand and supply as customers associate with smart microgrids, as well as expanding operational productivity, optimizing business activity, limiting unprepared downtime, and providing system secure. It gives applications like cybersecurity, predictive maintenance, and remote monitoring and optimizes business task, laborer well-being, and advanced distributed control [6].

To optimize the utilization of distributed energy resources (DERs), improve traditional grid infrastructure, and guarantee coordination with IoT, the grid needs to get more intelligent. A smart grid permits a bidirectional stream of electricity and communication between electricity providers and consumers. With a smart grid, buildings are changed from being comparatively passive loads on the grid to dynamic associates in the electricity sector, giving (possibly selling) electricity and trading data that takes into account load balancing to help a stable and reliable grid. Increased generation of energy requires extra adaptable and fast-ramping resources, for example, electricity storage facility to further resolve the possible vulnerabilities and discontinuity of utility-scale renewable generation. Transmission operators can account for assets and resources from the distribution and generation components of the grid. Operators can incorporate distribution while controlling essential tasks of the grid. Utilities may move toward becoming stages that offer grid infrastructure for third-party suppliers and aggregators that sell electricity and/or energy services.

Communication-enabled grid infrastructure bolsters optimization of distributed energy resources. A decentralized methodology brings the production near to required load, lessens transmission losses and vulnerabilities, and expands the general dependability, versatility, efficiency, and strength of the grid. Communication is bidirectional and closer to near-real time, empowering clients to be more likely oversee loads and expenses. Also, power rates might be progressively unique. Besides, intelligent building devices empower task of smart equipment by means of the Internet [1].

The smart grid bolsters the usage of more nuanced and successful demand management programs and the execution of progressively educated measures by the buyers. It likewise bolsters dynamic pricing, which could be a winning factor for consumers and utilities alike, enabling both to take more prominent favorable position of inconstancy on the grid, the wholesale electricity market, and DERs.

Intelligent digital meters, also known as “smart meters,” are fundamental to the smart grid. They empower bidirectional, near-real-time communication among buildings and a regional network about demand and supply. These meters can empower utilities to control loads more efficiently and thus guarantee greater grid dependability. Smart meters are likewise vital to consumers getting better, timelier data about utilization and pricing to advise options about loads and expenses. These decisions can likewise reduce load on the grids [1].

With the expanded spotlight on pollution-free energy and efficacy as well as the requirement to create the smart grid business system, an increasing number of stakeholders are focusing on smart microgrids as a practical and vital way to deal with an upgrade of the grid at the neighborhood level. The smart microgrids join the neighborhood energy supply to fulfill the correct requirements of the constituents alongside connecting with the bigger grid. These feature the scope of intelligent technology in a solitary area which boosts the quality of service and the creation of innovative occupation potential, and therefore, it helps to deliver a feasible business case. This helps in energy savings as well as cost saving to the customers. They additionally give neighborhood decision in regard to the source and supply of generating electricity [7].

Smart microgrids are an ideal method to coordinate renewable resources at the network level and take into account customer interest in the electricity venture [7]. Smart microgrids are like the smart grids. To optimize the utilization of renewable energy sources, these grids enhance consumer involvement infrastructure and guarantee to join with IoT at the network level. A smart microgrid permits a bidirectional stream of electricity and correspondence between electricity providers and consumers on the community level. To handle the problem of non-accessibility of individual renewable energy sources, IIoT performs an important task by monitoring the energy use, energy production, and its incorporation, particularly for the smart microgrid. Smart microgrids increase the local dependability through the foundation of an explicit dependability enhancement plan that incorporates the surplus distribution, intelligent switches, energy production, energy storage, automation, and other intelligent technologies [7]. With the upgrades and changes in the energy sector, utilities and energy market continually change for the future. However, with the changes such as expansion of DERs with an assorted variety of proprietorship including third-party suppliers that are not as intensely managed, that scaling is rather less. Nevertheless, the grid will keep on being important to the electricity sector [1].

In this chapter, we provide a detailed discussion of the concept, history, and applications of IoT. We also elaborate on changes coming to the energy sector, introduction to renewable energy, use of IoT in the energy sector, challenges of renewable energy sector, solution to the challenges using IIoT, and future of IIoT in the energy industry. This chapter also includes a detailed discussion of smart microgrids which are mainly based on renewable energy and IIoT concepts. It determines the role of IoT in smart grid and smart microgrid.

The chapter will hopefully help us to understand how an efficient IIoT-based energy system on renewable energy might work for improving the future in terms of better utilization of renewable energy resources as well as limiting the carbon

emission. This chapter also includes examples of IIoT-based projects in the energy sector on monitoring of energy usage and generation, especially in case of smart microgrid.

## 10.2 The Concept of Industrial IoT

This section articulates the basics of Industrial IoT including concepts, historical perspectives, benefits and challenges, as well as the literature review and future directions on the topic. In the later sections, we discuss the IIoT case studies in the energy sector.

### 10.2.1 *Definition and Benefits*

The IoT is a network of physical smart devices, home appliances, wearable and handheld intelligent devices, and various other “things” embedded with electronics, software, actuators, and sensors. It is a system of intelligent gadgets and items that share and gather enormous quantities of data. The gathered information is sent to a focal cloud-based service where it is aggregated with other data and afterward imparted to end clients supportively [5]. The IIoT (Industrial Internet of things) can be regarded as a particular application of the Internet of things (IoT) vision. Here, the interconnected devices of industrial nature communicate with each other over the Internet and can be controlled and supervised remotely [8].

The IIoT aims to modernize manufacturing and other industrial sectors by empowering the openness and acquisition of the large amounts of data, at far more prominent speeds, and with much more proficiency than previously witnessed. Various large organizations have begun to employ the IIoT by utilizing smart, associated devices in their factories [5]. The IIoT can extraordinarily enhance connectivity, efficacy, versatility, and time and cost savings for technologically based industries. Companies are now also profiting by the IIoT through predictive maintenance, enhanced security, and other functioning efficiencies. IIoT systems of smart gadgets enable industrial organizations to tear open information silos and join the majority of their workforce, company information, and operational processes from the plant floor to the official workplaces. Business pioneers can utilize the IIoT information to get a complete and precise perspective of how their venture is getting along, which will further enable them to make better choices [5].

### ***10.2.2 Historical Perspective***

In 1982, the idea of a system of connected intelligent gadgets was first put forward. In 1991, Mark Weiser, in a paper “The Computer of the twenty-first Century”, introduced the vision of device connectivity now commonly known as the IoT based on the concept of ubiquitous computing. Soon after, Bill Joy presented the idea of device-to-device (D2D) communication in what he called “Six Webs” system at the World Economic Forum held at Davos. The expression “Internet of things” was probably coined by Kevin Ashton of Procter and Gamble, and later by MIT’s Auto-ID Center, during 1999. At this point, it was also observed that radio-frequency identification (RFID) was a vital component of the IoT. This enabled computers to deal and communicate with many other single individual “things.”

An exploration article that mentioned the IoT was submitted at the meeting for Nordic Researchers in Logistics, Norway, in June 2002. The implementation portrayed therein was proposed by Kary Främling and his group at Helsinki University of Technology which became foundation for today’s data management frameworks. According to Cisco Systems, real developments in IoT began somewhere around the years 2008 and 2009, with the ratio of things versus individuals increasing from 0.08 in 2003 to 1.84 in 2010 [8].

### ***10.2.3 Challenges of the IIoT Vision***

One of the problems experienced in the progress of the IIoT is the fact that diverse edge-of-network devices have different communication protocols for sending and receiving data, for example, OPC-UA and the Message Queuing Telemetry Transport (MQTT). However, transfer protocols are rapidly developing toward standardization [5]. Interoperability and security are also the most likely the two greatest difficulties encompassing the deployment of IIoT. As technology author Margaret Rouse states, “a major concern surrounding the industrial IoT is interoperability between devices and machines that use different protocols and have different architectures”.

Organizations need to realize and be sure that their data is secure. The development of a diverse variety of sensors and other smart devices has also brought about a parallel blast in security vulnerabilities. This is another factor in the ascent of MQTT since it is an exceptionally secure IIoT protocol [5].

### ***10.2.4 Relevant Research Works***

A number of research approaches have been projected to utilize the IoT vision in the energy sector. Some of these are now discussed in this section.

In [9], the authors presented data collection architecture for situational awareness (SA) in connection with the microgrids. This work designed a prototype that can give huge amounts of information gathering capabilities relating to smart meters. An IoT stage is utilized for SA visualization by a customized dashboard. By the utilization of the proposed system, a satisfactory level of SA can be accomplished with a low establishment and equipment cost. Utilizing the proposed system, microgrid administrator can foresee all the obscure occurrences within the microgrid by means of gathering data from the smart meters from different consumers and administrators within the grid [9].

In [10], Kang et al. proposed an energy trading platform of blockchain-based smart homes in a microgrid. This paper explains the management of energy, transactions, and home miners in the blockchain-based smart home. The reported research presented a protected and computerized decentralized renewable energy exchanging stage inside the microgrid utilizing the block chain concept. In a blockchain-based smart home, it is difficult to forge data called transactions. By means of such transactions, the smart homes know the required data regarding energy consumption and requirement. By utilizing this data, they propose renewable energy exchanging stage utilizing Ethereum's smart contract to guarantee protected energy exchanging run consequently without the outsider intercession and involvement in a microgrid [10].

In [11], Roy et al. proposed a smart IoT-based energy metering system with load management algorithm for microgrids. This paper presented modifications in the bi-channel communication of the smart meters. The customary and ordinary utilization of the smart meters was seen as fundamental to set up a bi-channel communication: one channel to provide the pricing details of the energy utilization using GSM modules to the end clients, and the other channel to give energy-related information and other associated data that are of concern to the utility providers. There are two modifications discussed in this paper. Firstly, it focuses on the whole information into a single storage system, i.e., server, instead of utilizing two separate channels of communications. This helps both the client and the associated utility in getting access to the real-time data from any place on the planet. Secondly, this paper has made advancement in that the system automatically senses and secures loads from transients in lines (such as overvoltage, undervoltage, and overcurrent) with a load management algorithm using the smart energy meter IC. The proposed system consumes high power, requires consistent Wi-fi availability, and is restricted to single-phase microgrids—and these are its main drawbacks.

In [12], Aagri and Bisht explain the export and import of renewable energy by hybrid microgrid by means of the IoT. This paper gave an absolute, self-continuing, and open source solution for use of renewable energy by means of power grids. The paper also depicts the way to improve the hybrid power grid system in homes and to attach them to a central grid attaching numerous different homes. The node proprietors can buy and sell the produced/stored power in their homes, through utilizing a Web interface mechanism.

In [13], the authors proposed an IoT-empowered multi-agent system (MAS) for residential DC microgrids (RDCMG). The system comprises smart home agents (SHAs) that collaborate and help each other to mitigate the peak load of the RDCMG;

and reduce the energy prices for smart homes. These are accomplished by agent utility functions and the best operating time algorithm (BOT) in the MAS. The proposed IoT-enabled MAS and smart homes models were run on five Raspberry pi 3 boards and verified by experimental investigations for an RDCMG with five smart homes.

In [14], the researchers proposed a reliable control system dependent on the IoT to control and manage the flow of energy gathered by solar panels inside a microgrid. Information for reliable control incorporates measurements from neighboring sensors as well as meteorological data recovered in real time from online sources. For the fault tolerance of the system over the entire distributed control system featuring numerous controllers, reliable controllers are designed to control and optimize the tracking operations of photovoltaic arrays. This also maximizes the catch of solar radiation and keeps up the system flexibility and dependability in real time in spite of malfunctions of one or more redundant controllers (because of possible issues with communication, cybersecurity, and hardware). Experimental results are presented to verify the proposed methodology [14].

In [15], Saleem et al. provide a review of IoT-aided smart grids (SGs) systems, which incorporate architectures, technologies, applications, prototypes, and future research directions. They report challenges in the traditional grid due to which these are transformed into the smart grid. These challenges refer to a unidirectional flow of information and energy, energy wastage, increasing energy demand, dependability, and lack of safety. The power wastage occurs in traditional grids due to several factors, such as consumer inadequate machines, the absence of smart technology, ineffective routing, dispensation of electrical energy, unreliable communication and monitoring, and absence of energy storage system.

The conventional grid has operated superbly from its introduction in 1870 until 1970. By 1970, the consumer demand for energy also steadily increased, but it was predictable. However, a remarkable change in the nature of electricity consumption has occurred since 1970 because of the growth of the utilization of electronic devices and electric vehicles—this raised the demand for electrical energy tremendously. Furthermore, the demand for use of renewable energy sources also increased due to the impact of climate changes that forced the transformation of the traditional grid into a smart grid.

In order to combat the inherent challenges, smart grid technology was introduced. These grids can advance the efficiency, power quality, dependability, protection, scalability, and stability of the traditional grid. Smart grid reduces the energy wastage and optimizes the usage of electrical energy. These grids have capabilities of self-healing, real-time pricing, power consumption scheduling, and bidirectional flow of energy between service providers and customers. This is accomplished with the help of the IoT paradigm that helps smart grids in terms of connectivity, automation, and tracking of smart devices. These smart devices help in monitoring, analyzing, and controlling the grid [15–21]. The research in [15] also highlights the challenges, open issues, and future research directions of IoT-aided smart grid systems.

In [22], the authors proposed an IoT-based smart solar photovoltaic remote monitoring and control unit. Currently, the solar photovoltaic (PV) energy usage is increasing and it is one of the most attractive renewable energy sources. Due to the increase

in usage of rooftop solar photovoltaic systems, the need for monitoring of real-time generation is also rising in order to optimize the overall performance of the solar power plant. This also helps to maintain the grid stability [22, 23]. The generated power from the solar power plant is unpredictable in nature because of the changes in solar irradiance, temperature, and other factors. Therefore, remote monitoring has become an essential requirement. For installing a remote monitoring system in a solar photovoltaic system, IoT approach is used in the work of [22]. The remote monitoring removes the dangers linked to the conventional wiring systems. It also measures and monitors the data very easily and accurately; therefore, it makes the system more cost-effective. IoT-based systems help to intelligently monitor and control through the Web. This helps to increase the flexibility of deployment of the systems [22, 24].

Research in [22] has mainly proposed an IoT-based remote monitoring system for a solar power plant. This method has studied, executed, and successfully accomplished the remote transmission of information to a server for management purposes. The IoT-based remote monitoring system increases the energy efficacy of the system by utilizing the low-power-consuming wireless modules. This also diminishes the carbon footprint [22, 25].

### ***10.2.5 Future Developments in IIoT***

The IIoT is broadly viewed as one of the essential patterns influencing industrial businesses today. Enterprises are pushing to modernize frameworks and equipment to meet new directions, to stay aware of the expanding markets, and to manage problematic technology. Industries that have adopted the IIoT approach have seen huge upgrades to security, effectiveness, and benefits, and it is normal that this pattern will continue as IIoT technologies are all the more broadly embraced. The ignition IIoT remedy extraordinarily enhances connectivity, productivity, adaptability, time savings, and cost savings for industrial companies. It can likewise enable enterprises to get most value from their framework without being obliged by financial and innovative restrictions. Due to these reasons and more, ignition offers the perfect stage for bringing the power of the IIoT into further undertaking [5].

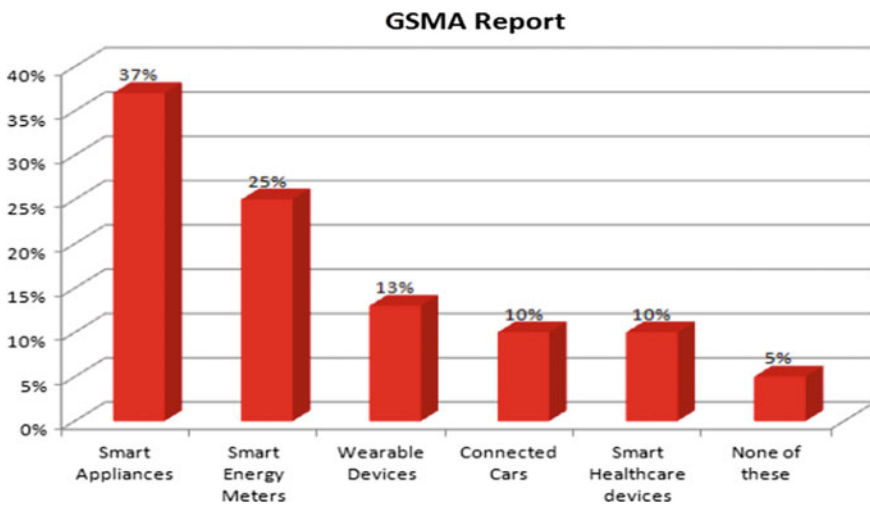
The IoT can encode 50–100 trillion items along with the ability to pursue the movement of those items, e.g., in smart transportation. In urban situations, each network is encompassed by 1000–5000 trackable items. In 2015, 83 million smart devices were previously present in a typical home. This figure is heading for an increase of up to 193 million gadgets in 2020. It will obviously continue rising perhaps exponentially. The figure for online competent gadgets became 31% from 2016 to 8.4 billion in 2017 [8]. The IoT's major critical pattern in current years is the explosive increase of devices controlled and connected by the Internet. An extensive utilization of this technology implies that the points of interest can be altogether different, starting with one gadget, then onto the next; however, there are several fundamental attributes of these devices shared by most. Internet of things makes it straightforward for the more straightforward mix of the physical world into

computer-based systems, bringing about product upgrades, financial advantages, and decreased human efforts. The quantity of IoT devices has expanded 31% every year; now toward 8.4 billion in the year 2017. It is expected that there will be expansion of up to 30 billion gadgets by 2020. The global market estimation of the IoT is anticipated to arrive at \$7.1 trillion by 2020 [8].

This latest level of connectivity within the IoT is going past the laptops and smartphones. Connectivity is now across connected cars, smart homes, connected wearables, smart cities, and connected healthcare. Fundamentally, it is presently intended for a connected life in connected environments. As indicated by a Gartner report, connected gadgets will reach around 20.6 billion by 2020 [26]. HP recently completed a review in which they evaluated the increase of connected devices throughout the years and the outcomes are astounding. These being that:

- In 1990, there were 0.3 million connected devices.
- In 1999, the number increased to 90 million.
- In 2010, there were 5000 million connected devices.
- In 2013, connected devices increased in number to 9000 million.
- In 2025, there will be around 1,000,000 million devices.

This level of connectivity will overcome any issues among physical and digital worlds to enhance the quality and efficacy of life, society, and industries [26]. Utilization of IoT in smart homes is the most anticipated development, with new brands entering into the competition with yet smarter appliances. The second trending feature of the IoT vision is intelligent wearables. An analysis, as shown in Fig. 10.1, directed by KRC research in the UK, USA, Japan, and Germany, the early adopters of IoT, has exposed which gadgets are the most consumers bound to use in the coming years. Smart appliances like thermostat, smart refrigerator, etc., are some examples



**Fig. 10.1** GSMA report results



which are mostly enjoyed by the consumers and are appearing to change the manner in which human individuals live and operate [26]. This analysis in Fig. 10.1, supported by GSMA, also indicates that smart devices will play a crucial role in the future to further improve the world through the Internet.

In summary, to comprehend the effect of the IoT on the economy according to the CISCO report, IoT will produce \$14.4 trillion in value over all industries in the upcoming decade [26].

Industrial Internet, i.e., IIoT, is the latest buzz in the industry sector. It is enabling industrial engineering with sensors, software, and big data analytics to build smart equipments and environments. The driving factor behind IIoT is that smart equipment is more exact and predictable than humans in communicating the information. Furthermore, accurate and timely information can enable organizations to notice ineffectiveness and limitations quicker. IIoT holds extraordinary potential for quality control and maintainability. As indicated in Gartner report, the enhancement of industry productivity will create \$10 trillion to \$15 trillion in GDP worldwide over the next 15 years [26].

A smart city is another incredible illustration of the use of IoT creating interest among the world's population. Smart supervision, automated transportation, smarter energy management systems, water distribution, urban security, and environmental monitoring are some of the other related applications of the Internet of things in relation to smart cities. IoT will also take care of other significant city-related issues such as pollution and traffic jamming [26].

### 10.3 Applications of IoT

There are various applications of the IoT paradigm, especially in the fields of consumer requirements, commercial, industrial, and infrastructure domains. IoT devices are used within vehicles, home automation, wearable technology, connected health-care gadgets with the ability of remote monitoring. Smart devices are used in lighting, media, safety, heating, and air-conditioning system for saving energy expenses through automatic controls. IoT-based homes, also known as smart homes, are helpful in controlling smart devices as well as being helpful in taking care of those with inabilities and elderly people.

IoT plays a crucial role in medical and health-related domains and also information gathering and examination of research and checking. IoT-based devices are helpful for health observation, for monitoring blood pressure and heart rate, for example. IoT-based devices are also used in smart beds to provide further patient care in the hospital. These beds mainly help hospitals by sensing that the patient is trying to get up or is in difficulty.

IoT-based devices empower faster manufacturing of new items. It empowers real-time optimization of the manufacturing industry. The smart industrial systems can be incorporated with the smart grid to empower real-time energy optimization. IoT-based devices are useful in farming and also for gathering data on temperature,

rainfall, the speed of the wind, humidity, pest infestation, and soil content. This information is utilized in robotized farming techniques for taking educated choices to enhance the amount and quality of crops. It helps to minimize danger and waste. With the help of IoT devices, farmers are now capable to check soil moisture as well as temperature from a distant location. IoT devices can be used for checking and analyzing air quality, water quality, atmospheric conditions, and soil conditions. This helps in reducing water and air pollution especially. Such devices can be used to observe movements of wildlife and their inhabitants [8]. IoT-based devices can also check the structural conditions of infrastructure for avoiding future danger from a distant location.

IoT-based connected devices increase and promote paperless work processes and help to increase the efficacy of the construction industry. This improves work quality. IoT devices help to build a communicative relationship between energy-consuming devices and utilities using the Internet, which in turn enables to adjust energy production and energy consumption and also to optimize for savings in energy bills. IoT helps in monitoring different components of the smart grid and smart microgrid including consumer meters. This enhances security and helps in fault detection and correction.

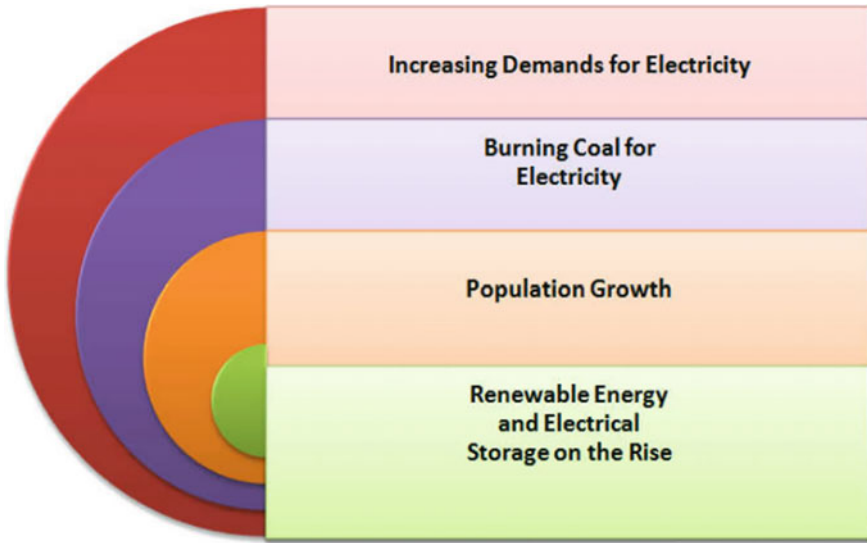
## 10.4 Changes in the Energy Sector

This section looks at the changes and developments taking place in the utilities sector, especially the energy sector.

### 10.4.1 *Reasons for Such Changes*

New advancements and emerging methodologies are bringing huge changes in the electricity sector. Figure 10.2 illustrates some of the significant causes for such changes. Underlying reasons include: increased demand for electricity, new approaches to production of electricity, increase in population, and the attraction of renewable energy, together with the storage of energy. Currently, 85% of the world population uses electricity. Buildings utilize 60% of electricity worldwide, and buildings in the developed world utilize over 70% of electricity. By 2040, 33% of all vehicles are anticipated to be electric [1]. With the passing of time, demand is on the rise.

By 2050, the world population is expected to rise to 9.7 billion, of which 66% are expected to live in cities. Expanding urbanization will result in the construction of new cities, each on average about the size of Singapore (currently, population of 5.8 million) every month until 2050 [1]. Presently, 40% of world electricity originates from burning coal; and this contributes 70% of the carbon dioxide (CO<sub>2</sub>) emissions from electricity generation. Coal contributes to the kind of emissions that are more



**Fig. 10.2** Major reasons behind changes coming to the electricity sector

dangerous to the environment and human health than other fossil fuels. It is in order to reduce these emissions that the utilization of renewable energy and its storage is rising. Renewable sources of energy (biomass, hydropower, geothermal, wind, and solar) are the world's fastest-growing new energy production resources. Battery technology is also enhancing, and the associated costs are reducing [1].

Based on these facts, it is clear that there are reasons for changes and further beneficial developments in the electricity generation and supply sector. Since electric lights firstly showed up in buildings, the electrical grid and buildings have had a critical relationship. This relationship is mainly one-sided: The grid provides electricity, and the buildings are passive consumers. Nonetheless, new technologies and methods to reduce energy costs and the environmental impacts of electricity (produced from fossil fuel) are quickly changing the way the buildings communicate with the electrical grid. Additional factors for the change incorporate technological advancements and falling costs in renewable energy technology, batteries, sensors and controls, remote access technologies, and building management systems [1]. For controlling, overseeing and accomplishing these two-sided communications with new technologies, IIoT plays a vital role, particularly due to the emerging new renewable energy technologies.

### 10.4.2 The Electrical Grid Today

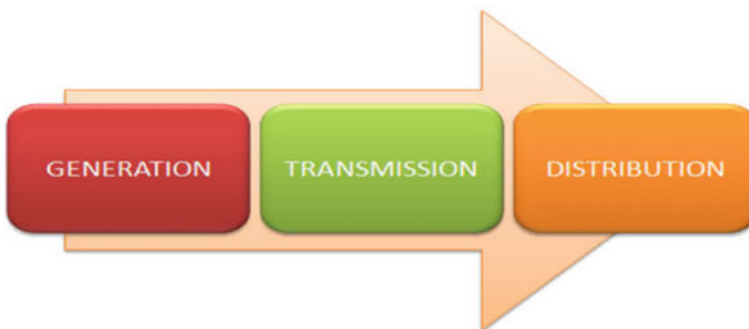
The present-day electrical grid model has served those with access to electricity, exceptionally well for quite a while. In spite of the fact that the model is transforming, it is essential to comprehend the systems that got us to where we are today. The provision of electricity generally depends on three key segments: generation, transmission, and distribution. Figure 10.3 demonstrates the flow of electricity in the traditional electrical system.

Conventionally, utilities produce or purchase electricity in bulk from centralized power plants located a long way away from end buyers. Conventional generation comes mainly from thermal plants (fossil fuel, nuclear, and geothermal) and hydroelectric projects. Wind and solar technologies, including solar thermal and electric, also contribute, but these are still at development levels of generation [1].

In today's electrical grid, the thermal power plants (not including solar thermal) are just about 30–40% productive and are noteworthy contributors of carbon and pollutant emissions. Generation resources are of two varieties: baseload resources and peak generation resources. Baseload resources are those that cannot be effortlessly ceased and begun (e.g., coal, hydroelectric, and nuclear). Peak generation resources give short-term and variable production capacity over the baseload resources to take care of peak demand. Peak demand is a period of time (e.g., time of day or season) during which customer demand for electricity is at the highest, or at its "Peak". A choice about which peak generation asset to set up is commonly made on cost. However, more recently, it is likewise being organized dependent on environmental and sociological impact [1].

After production, electricity voltage gets stepped up and transmitted over a long distance to progressively local distribution, where the voltage is stepped down and provided to consumers. For transmission, this happens over a long distance with about 5% of electricity in line losses.

The present electrical grid was intended to satisfy twentieth-century demand. Power flows in one direction (i.e., provider to consumer), and there are no data trade between electricity providers and consumers. Grid infrastructure is intended for one-



**Fig. 10.3** Flow of electricity in the traditional electrical system

route stream of electricity from generation through transmission and distribution to end customers [1].

Operational control and communication excludes the customer side of the meter and frequently exclude distribution infrastructure. Communication with the customer is one way. For bigger purchasers of electricity, charges for generation, transmission, and distribution generally appear on their bill. At the residential level, the three expenses are frequently combined into one. Utilization and cost information are commonly given in the aggregate every month, constraining the capacity to determine what drives costs and consumption over the charging time frame. To the extent that communication from consumer is concerned, a utility typically does not know that there is an issue to the point when the customer calls to report an outage, etc. [1]. This just shows the basic infrastructure of the current electrical grid, and its generation and supply scheme.

### ***10.4.3 The Buildings Today***

Buildings consume over 70% of the electrical load in developed countries. Grid loads from buildings vary by changing season and due to climate changes that can occur quickly, as well as due to activities inside the buildings. The traditional electrical grid puts the burden on the grid to give dependable generating capacity and a transmission and distribution system that reacts to load changes promptly and takes care of peak demand. Although buildings and the grid do not communicate, the grid is required to meet building demands whatever the situation [1].

The business models of the electricity sector are focused on selling electricity. However, from an intended and infrastructure investment perspective, they do not want consumers to purchase everything in the meantime. Without the capability to speak with customers about loads, utilities have created expense structures to send signals to customers to utilize electricity steadily with the efficient operation of the grid infrastructure. These expense structures can include three variables: Time of use rates, demand charges, and ratchets. Time of use rates is the cost of electricity changes depending on the time of day. Demand charges, based on real-time power usage (over a period of time: regularly month to month), are extra charges levied depending on peak demand in kW for the considered periods of time. Ratchets are like demand charges, yet they consider the peak consumption for a yearly period of time. These customary expense structures impact the design and activity of buildings. For instance, thermal storage might be utilized to move cooling loads. While this decreases peak load electricity charges, it can permit to utilize more energy generally. At the point when fossil fuels are utilized to create power, this sort of load moving can result in excessive amounts of carbon emissions and different pollutants [1].

A building automation system (BAS) might be utilized to restrict demand charges. The BAS monitors the peak electricity usage by the buildings and can shed interior loads (e.g., reset room temperature, or switch off lighting) to remain under a suggested electricity demand. In any case, without two-way communication between

the building and the grid, these measures can occur only on days when there is no requirement of decreased loads to assist the grid. Planning, developing, and executing a building that foresees potential electricity expense structures without grid communication can prompt superfluous occupant inconvenience and increase in emissions [1].

All things considered, utility demand response programs have started to close the gap caused by the absence of communication among utilities and consumers. The utility and consumers enter into a relationship in which, under certain characterized conditions and specialized strategies, the utility suggests incentives to diminish or move loads. At the point when the utility decides that a load decrease is required, the consumer is informed. The notification may happen, for instance, in expectation of higher demand; BAS may slow down or shut down a predetermined system. The signal could likewise be automatic. Generally, the activity of the building does not always align with the utility objectives. Demand response is a genuine precedent in which objectives are adjusted, while energy efficiency measure is a progressively more unpredictable subject [1].

The conventional business plan for utilities, selling electrical energy to be beneficial, clashes with energy efficiency; yet utilities are frequently required by government policy and regulators to subsidize customers to execute and work with such energy-saving measures. Citizens, government, and regulatory entities around the world enact policies to support more noteworthy energy efficiency and utilize renewable energy and the decrease of carbon emissions and different pollutants in the electrical and building sectors. These policies influence making of decisions in the two sectors: decisions that influence costing mechanisms for the utility providers, and decisions that influence consumption by the customers. It is significant that in the USA, 80% of the decrease in carbon emissions in 2005–2016 originated from the electricity sector. Despite the fact that policies regularly command utilities to execute energy efficacy programs, some policies additionally support energy efficacy as a way of guaranteeing production capacity without putting resources into new power plant development and activity. However, utilities regularly battle with out-of-date business models that clash with the necessities of consumers and societal values around the effective utilization of resources and the environment [1].

#### ***10.4.4 Development of Zero-Energy Buildings***

Zero-energy buildings (ZEBs) are a precedent for building structures that are driven by societal ethics around energy efficacy and renewable energy. The structures both react to and put stress on the present grid model. The Department of Energy (DOE) of the USA gives a basic description of a ZEB, that is, an energy-efficient building where, on a source energy premise, the genuine yearly delivered energy is not exactly or equivalent to the on-location renewable exported energy. Here, source energy incorporates all the generation, transmission, and distribution losses in the electrical energy delivery to the buildings. Electrical energy is produced on-location

for renewable energy, for example, solar photovoltaic (PV). But the building may even now require electrical energy from the grid on occasions, except if the battery storage is accessible on the building location. At the point, when the renewable production or battery storage (or both) do not meet building loads, the grid fulfills the additional requirement. At the point, when excess renewable energy is created, it might be sent to the grid [1].

The US DOE ZEB definition has been extended further, to incorporate zero-energy campuses, communities, and portfolios. This resulted in a few difficulties at first noticed by ZEBs. For example, the necessity for on-location renewable production restricted various environmentally benevolent alternatives such as power purchase agreements and community solar. Also, the on-location production measure disheartened urban density, contributing to undesirable sprawl, which can likewise result in poor walk capability. With the growth of the ZEBs, the “on-site” would now be able to be characterized as a gathering of building destinations in an explicit region that have renewable production and that are claimed by a single entity or numerous entities or that are rented by a single entity [1].

ZEB plan offers a solid way ahead for an environment that advances the health and prosperity of the inhabitants while increasing energy efficacy and utilizing renewable energy options. All things considered, the vision must keep on progressing to some degree in view of the fact that ZEBs may not be very much lined up with the necessities of the electricity sector. For instance, if the on-location production fails, the expectation is that the utility will still provide the required power. But the reality is that utility gets paid to provide electrical energy, not reliability. In numerous locations, the utility is required to accept and pay for surplus power from the ZEB, regardless of whether it is or is not accessible when the utility needs it. Sharp deviations in ZEB load profiles can be troublesome for the grid to handle. Sometimes, electrical energy peak demand corresponds with decreases in the renewable production (e.g., in late summer afternoons when cooling loads peak yet solar PV production starts to diminish). This can result in a lofty increase in demand for power. Furthermore, the movement of electrical energy onto the grid from on-location production was not part of the preliminary grid structure. In view of the above, changes in grid infrastructure, utility business models, and building load management become essential to adjust electrical energy and building sector needs and provision [1].

High-performance, low-energy-use buildings are vital for our future, and especially in the smart homes scenario. Therefore, ZEBs will play an imperative role. The ZEB definition has been and will keep on developing and encompassing more to help accomplish the superior objective of high performance. Aligning the objectives and concept of ZEBs with the objectives of the electrical energy sector, particularly as utilities advance in view of changing customer demands and emerging new technologies, will necessarily drive positive outcomes [1].

## 10.5 Renewable Energy and IoT in the Energy Sector

This section has a focus on renewable energy vision. The following subsections discuss in some detail the underlying concept along with developments in electric grids. Applications of the IoT, including developments on electrical vehicles, are also presented.

### 10.5.1 Renewable Energy

Societal demand for renewable energy is increasing, while the cost for the relevant technologies is coming down. So, the utilization of renewable energy for electrical energy production is only expected to increase; however, the utilization of renewable puts a strain on the current electrical grid system. The advantages of renewable energy are clearly evident for both the building owners and the electricity sector. The building owner can diminish energy expenses by selling surplus renewable electrical energy to the utility company or utilizing net metering to get a credit from the utility for excess electrical energy produced by renewable systems. The utilization of renewable energy likewise lessens the emissions associated with the buildings. The utility may likewise have the benefit of decreased peak demand and evade expansive capital investment in new ways of generation and transmission. Utilities likewise would also construct large-scale wind and solar farms to enhance their production resources [1]. There is no doubt that full advantages of renewable electrical energy are increasing and the vision is becoming more attractive.

The conventional grid was intended for steady flow of electrical energy from the high-quantity base load and not intended to accommodate broadly distributed, smaller, and discontinuous (not constant) production from sources such as solar PV and wind. Additionally, transmission and distribution assets were intended to move electrical energy from remote production to customers. They were not intended to empower one building to impart surplus capacity to/from another close-by building. Besides, the present grid is not intended to successfully monitor and deal with the huge amounts of bidirectional flows of electrical energy that are simple to envision as the demand for and viability of renewable electrical energy grows. Dealing with a huge and scattered number of production resources with a diversity of owners is even more difficult. Electrical energy flows from high voltage to low voltage; therefore, for surplus electrical energy to move out of a building back to the grid in turn, this also required the voltage to be raised above grid voltage. With an extensive number of production resources that are not under the operational control of utilities, the grid rapidly keeps running into voltage issues [1].



### ***10.5.2 Electrical Grid in the Era of the IoT***

The conventional grid infrastructure is now changing with the emergence of new technologies, more efficient methods, and emphasis on ZEB configurations. Additional technological changes and rising demands are also being projected to drive much more change to the physical grid and compel utilities to employ new business models, possibly changing the fundamental market requirements of electrical energy. In the generation sector, grid infrastructure is intended for vast, controllable production and one-way flow of electrical energy. In this sense, solar and wind resources are irregular. Without storage, they can disturb the stable maintenance of demand and supply. In the transmission sector, utilities sell electrical energy for earnings and profits. Utilities keep up a grid infrastructure to empower the delivery of their products. Proprietors of DERs (Distributed Energy Resources) may not purchase as much electrical energy as other consumers; however, in the distribution sector, electrical energy is presently being provided from the distribution part of the grid, requiring a bidirectional flow of electrical energy. Net metering empowers bidirectional flow of electrical energy from limited distributed production and yet may not be the main answer for higher infiltrations of distributed production. In the communication sector, operational control and communication does exclude the consumer side of the meter and frequently does exclude distribution infrastructure. Communication with the consumer is one way and does not utilize the grid network infrastructure. It is utilized just for the unforeseen events, for example, power outages.

Changes in the electricity sector will open doors for its customer as well as the building sector. Technical changes predicted to affect the two sectors incorporate DERs (of which distributed production of renewable energy is a key segment), an expansion of plug-in electric vehicles and transportation sector as well as the generic IoT and the smart grids [1].

### ***10.5.3 Distributed Energy Resources (DER)***

Distributed energy resources (DERs) are a noteworthy element of progress for the electrical grid. The traditional grid was intended for centralized generation and one-way flow of electrical energy. DERs change that by installing generation assets on the distribution segment of the grid and compelling bidirectional flow of electrical energy. DERs are mainly related to buildings. It is therefore essential for building professionals to inform themselves and their clients about DERs since DERs signify critical technologies and strategies through which buildings advance from passive consumers to dynamic partners with the grid. DERs are also termed as: distributed energy systems, distributed generation, and distributed power. The propensity is to consider DERs simply physical resources (e.g., solar PV, wind, batteries), yet DERs incorporate virtual resources, for example, plans to diminish or better supervise loads [1]. DERs include distributed generation, community solar, electric storage, nano-

grids, microgrids, third-party providers, third-party aggregators, and plug-in electric vehicles.

Here, distributed generation is comprised of a small number of electric generating units, from 3 kW to 50 MW. These smaller-scale power sources (as opposed to large utility scale) are well situated to electrical grids. They are, generally, “behind” the meter on the customer side and near to the loads for which they give power. These power sources can be linked to the grid, or they can be stand-alone; the output from various units can be collected to take care of the standard electricity demand.

Distributed generation challenges the centralized generation model of the current grid and is the main thrust in changing the model of the grid from one-way to bidirectional electricity flow [1]. Some examples are: Solar PV (including rooftop solar arrays, building integrated photovoltaic, on-site ground-mounted solar arrays), wind turbines (including utility scale larger than 100 kW, small wind 100 kW and smaller and offshore wind), generators (utilizing diesel, oil, natural gas, or a combination of fuels), co- and tri-generation, fuel cells, microturbines, and reciprocating engines.

Solar community is a business infrastructure for distributed renewable production in which electrical energy is generally produced off-site (i.e., not on a building or building site) and gives power relative to the number of customers it serves. This is especially advantageous to consumers who need solar PV for an assortment of reasons [1].

Electric storage choices incorporate batteries, even those used in electric vehicles. Electric storage can help balance the grid and make it increasingly adaptable. It can be utilized when generation surpasses demand, and the stored energy can be discharged to fulfill demand at some other time (e.g., when intermittent renewable production is not fulfilling demand). Otherwise, when a short-term peak in demand happens, storage can lessen the requirement for short-term peak generation, which is frequently the most costly generation [1].

Nano-grids and microgrids are smaller nearby electrical grids that utilize distributed generation and incorporate advanced controls and battery storage. Their distinction is one of scale:

- Nano-grids are smaller in size than microgrids, frequently residential or single building. They normally utilize solar PV for the generation, batteries for storage, and on-location “grid” components.
- Microgrids are bigger, campus or multi-building in scale and utilize a more widespread array. Sometimes, they utilize an integration of generation technologies (e.g., solar PV, wind, combined heat and power generators) and storage. Their grid components are typically not situated nearby to a single building, but rather regularly require their very own devoted space. They empower numerous buildings to share electrical energy and storage.

Nano-grids and microgrids are connected to the bigger electrical grid at a point of basic coupling that keeps up the voltage at an identical level from the primary grid and adjusts the frequency except if there is motivation to disconnect (e.g., outage or need to control electricity flowing back onto the grid). A switch can isolate the nano-grid or microgrid from the primary grid automatically or physically, and the smaller

grid at that point works separately as an island (called “islanding”). Nano-grids and microgrids offer benefits to utilities as well as to customers. They can give backup power in case of grid failure [1].

Third-party providers and third-party aggregators perform a critical job in DERs. Third-party providers offer a variety of products and services to buyers and utilities. Aggregators offer products and services of various third-party providers. These products and services are dispersed across the grid and incorporate the following: distributed production, at times, combined with storage; energy efficacy products and services; billing software and services; energy management services; grid dependability products and services for utilities [1].

#### ***10.5.4 Plug-in Electric Vehicles***

Plug-in electric vehicles perform a critical role in transforming the electric grid. Overall utilization of electric vehicles (EVs) is estimated to increase from about 1% of the global light-duty fleet today to about 7% by 2030 and 33% by 2040. EVs indicate both the difficulties and opportunities for the electrical grid and buildings. From the grid viewpoint, EVs are regarded as a noteworthy factor in the increase in overall demand for electrical energy. As they confront selling less and less electrical energy, utilities might look more favorably at electrified transportation sector as a genuine advantageous factor for their business model. From the buildings point of view, EV proprietors hope to establish means for charging these vehicles at home, at work, and in public locations [1]. The beneficial impact of this change on buildings include the following: benefits to the owners of EV by way of charging; converting a fossil-fuel-based fleet to electric mode of transportation; EV charging incentives; and future EV charging requirements and desires. For the electrical energy and buildings sectors, EV charging can possibly essentially change the load patterns. The energy stored in EVs offers steadiness to both the grid and the buildings, particularly in case of distributed generation. EVs can, for instance, counterbalance the discontinuity of solar PV or wind power by charging around midday or at night when these resources are at their peak production, separately. EVs can likewise limit frequency and voltage fluctuations during grid interruption, profiting both the electricity providers and the consumers. Additionally, with dynamic pricing as an alternative, the owners of EVs could charge batteries when demand and prices are low, and then sell electricity back to the grid at a more expensive rate when demand spikes. This avoids grid overload [1].

### ***10.5.5 Other Applications of the IoT***

In addition to DERs, the electrical and buildings sectors will see changes from the expanding IoT, as already mentioned. Since IoT is a system of interconnected every-day devices, appliances, and objects fitted with computer chips and sensors (that can gather and transmit data through the Internet), we can apply this idea to commercial buildings, and then, we have Buildings IoT (B<sub>IoT</sub>). Buildings IoT devices can contribute to much smarter and more energy-efficient activity of building apparatus and devices, for example, in relation to HVAC, lighting, and security. Generally, buyers are now implementing IoT vision that associates with both the electricity sector and residential buildings. Numerous products are already available that offer Internet-enabled controls for household functions (e.g., lighting, HVAC, home safety, etc.), to make their living environments as smart homes. IoT devices are likewise commonly changing human anticipation regarding the speed and effortlessness with which we can control our immediate environments (e.g., tone and color of led lighting, home entertainment alternatives, speaker volume), which can possibly affect the electrical energy and buildings sectors [1].

A couple of speculative conceivable outcomes are worth taking into account. Even though numerous IoT device manufacturers' guarantee energy savings, these devices could really result in more noteworthy utilization of electricity and change load patterns just on the grounds since they make the task of electric equipment so natural and trouble-free. IoT devices may likewise change assumptions regarding the assortment and granularity of data. For example, without data on the explicit electric load of HVAC equipment, which can be hard to discover in a few buildings, such a suspicion cannot be affirmed. We have smart watches that track biometric data such as heart rate and sleep quality to enable us to examine our health. It is conceivable that building occupants may want to effortlessly contrast biometric information and data about building activities, for example, lighting levels and color to decide the effect of those measures on health [1]. However, as said before, without enough appropriate data, the afore-mentioned suspicions cannot be affirmed.

Utilities intend to further utilize IoT-based devices to enhance business and grid tasks. They are likewise anticipating to give services companionable with IoT devices to enable purchasers to all the more likely deals with their loads and in this manner reduction in their expenditure. This enables utilities to oversee generation, transmission, distribution, and loads in a much better way too. At the end of the day, the IoT could turn into something by which utilities "can see" loads and cooperate with buildings inhabitants to deal with those loads in the future [1]. IoT can enhance occupant comfort, support health and wellness, promote energy efficacy efforts, and facilitate the utilization of cloud computing infrastructures. Those are only a few instances of how IoT can team up with buildings environment. Similarly, as smartphones and intelligent devices are changing human expectation about the speed and security of data and the capabilities to get support with daily activities, the IoT vision needs to change the desires for buildings occupants and buildings activities [1].

### ***10.5.6 IoT/IIoT-Based Electricity Generating Project Examples***

There are several examples of projects that embed the required changes as suggested above and utilize latest technologies.

Jacobabad Institute of Medical Sciences in Sindh Province, Pakistan, is one such project. This institute has around 130 beds, occupying around 115,000 ft<sup>2</sup> (107,000 m<sup>2</sup>) and overall spread over around 8 acres (3.25 ha) of space. It incorporates rooftop solar PV that produces approximately 490 MWh/year via a two-bank battery system, 6900 and 20,700 Ah [1].

The Sacramento Municipal Utility District (SMUD) and Sunverge Aggregated Distributed Energy Storage and Solar PV in California, USA, is another such model. SMUD and Sunverge Energy cooperated to assess how high infiltrations of renewable electrical energy generation could yield better outcomes with consumer-sited energy storage. In 2016, around 28% of electrical energy created in California originated from a blend of renewable fuels, and the maximum level of the blend was about 10% solar. The state has a policy mandate that half of the produced electrical energy will originate from renewable fuels by 2030, and solar is estimated to make up the biggest level of the blend. The SMUD/Sunverge project incorporates a mix of 2.25-kW PV installations and 11.64-kWh Sunverge Energy Solar Integration Systems (SIS) installed in 34 houses. The SIS incorporate lithium-ion batteries (versatile from 7.7 to 19.4 kWh), a hybrid inverter (adaptable to 6 KW), and advanced controls software and electronics that Sunverge guarantees will convey power at the opportune time and the most minimal conceivable cost [1].

Pura Energía and sonnen are solar plus storage microgrids in Puerto Rico is another such precedent. Su Matrullas is a school providing kindergarten through Grade 9 education for around 150 students in a remote, mountain community in southern Puerto Rico. Indeed, even before Hurricane Maria struck Puerto Rico in September 2017, utility grid services were not dependable. After the hurricane, grid services were absent. The solar company Pura Energía and a US backup of the Germany Company Sonnen worked with other public and private party sources to set up an off-grid solar plus storage microgrid system. It comprises a 15-kW solar PV array, one 4-kW and one 8-kW battery (both lithium ion with inverters), and a backup diesel generator. Expectation is that the microgrid system will give electrical energy to keep the school open and fully operating; the school does not plan to interface with the bigger grid [1].

## **10.6 IoT in Smart Grid and Smart Microgrid Sectors**

This section is focused on discussions on smart grids and smart microgrids. We also present project examples and application scenarios.

### ***10.6.1 The Smart Grid***

To optimize the utilization of DERs, enhance overall grid infrastructure, and authentically connect with the IoT, the grid needs to be more intelligent. A smart grid permits a bidirectional flow of electrical energy and communication between electrical energy providers and customers. With a smart grid, buildings are changed from passive loads on the grid to active partners in the electrical energy sector, giving (possibly selling) electrical energy and trading data that permit load balancing to maintain a stable and reliable grid. In the generation sector, the bulk production is developing to greener sources, for example, renewable energy and natural gas. Production incorporates progressively adaptable and quick-inclining resources and mechanisms, for example, electrical energy storage system to keep up with the uncertainty and discontinuity of utility-scale and distributed renewable production. In the transmission sector, the transmission operators can utilize assets and resources from the distribution and bulk production parts of the grid. Operators can incorporate distribution while controlling grid activities. In the distribution sector, the utilities may move toward becoming stages that offer grid infrastructure for third-party suppliers and aggregators that sell electrical energy or potential energy services. In the communication sector, the optimization of distributed energy resources is supported by the communication-enabled grid infrastructure.

A decentralized methodology brings production nearer to load, diminishes transmission losses and vulnerabilities, and enhances the overall dependability, flexibility, and stability of the grid. Communication is bidirectional and nearer to near-real time, empowering clients to more readily oversee loads and expenses. Electrical energy rates might be progressively dynamic. Smart building devices empower the task of smart equipment by means of the Internet [1].

The smart grid bolsters the usage of more nuanced and efficient demand management programs by the utility and also bolsters the execution of more educated measures by the customers. It additionally strengthens dynamic pricing, which could be a win for customers and utilities alike, enabling both to gain benefits of inconsistency in the grid, the wholesale electricity market, and DERs. Smart digital meters are important to the smart grid. They empower bidirectional, near-real-time communication between buildings and an area network about demand and supply. These meters can empower utilities to control loads more efficiently and in this way guarantee superior grid reliability. Smart meters are likewise important to buyers getting more accurate and timely data about users and electricity usage and to notify users of alternatives about loads and costs. These alternatives can likewise lessen the load on the grid. Even though numerous buildings utilize BAS and energy management software that provides them with insights into variable loads and expenses, most customers do not have the advantage of such frameworks. Without smart meter technology, these buyers have no method to monitor those sorts of fluctuations [1].

Smart equipment and appliances additionally use sensors and software to communicate by means of an area network. Through a smart meter, utilities might have the capability to speak with smart equipment and appliances to control loads. This would

need a transfer in the present-day utility–customer relationship. The customer would enable the utility to control loads on the customer side of the meter. It remains to be seen to what degree this transfer would be perceived as an undesirable interruption or a societal advantage that advances the execution of the electrical infrastructure. Customers can likewise utilize smart equipment and appliances to improve control time of activity to exploit the accessibility of more affordable electricity. Smart meters, equipment, and appliances can be linked to client interfaces that visualize data about energy supply, loads, and expenses and empower educated choices about which loads to include and when. The interface would likewise enable utilities to communicate in near-real time with consumers about any utility-controlled loads or outages [1].

As an ever-increasing number of buildings with distributed generation are on the grid, it is generally helpful to the proprietors of DERs and the utilities to work on a smart grid. Renewable electrical energy is irregular, yet it may be planned with an assorted variety of frameworks (e.g., solar, wind, and biomass) to lessen irregularity and fulfilled base load demand. A smart grid enables the utility to improve grid tasks to take full benefit of accessibility of electrical energy from irregular sources, which might be claimed by the utility, the client, or another third party. A smart grid could empower the non-utility proprietor of electrical energy and the utility to set up a strong business relationship that enables the proprietor to sell its electrical energy and the utility to purchase that electrical energy or distribute it on the grid for others to purchase.

The smart grid also faces a few difficulties. At the point when the electrical grid incorporates bidirectional flow of electrical energy, the assignment of keeping that electrical energy from hurting workers, people on the call, and building occupants turn out to be all the more challenging. Interoperability is another key problem faced by the smart grid, which will incorporate expanding quantities of DERs and DER owners; smart buildings, equipment, appliances, and electronic devices; and progressively refined communications. Interoperability is the capability of these components (networks, systems, devices, and applications) to cooperate viably and trade and use data safely without causing bother or issues. The smart grid supports and confronts resiliency in buildings. To maintain resiliency, for instance a preference for life, well-being and crisis structures can be incorporated within the electrical grid. Nevertheless, cybersecurity concerns must be considered to guarantee resilience [1].

### ***10.6.2 The Smart Microgrid***

With the growing attraction of pollution-free energy and efficacy as well as the requirement to create the smart grid business system, an increasing number of stakeholders are concentrating on smart microgrids as a practical way to deal with an upgrade of the grid at the neighborhood level. These grids are mainly created for a community e.g., college, school, or other similar environments. The smart microgrids join the neighborhood distributed energy supply to fulfill the correct requirements of the constituents alongside connection with the bigger grid. It includes the scope

of intelligent technology in a solitary area. This boosts the quality of the service and helps in the creation of innovative occupations. Therefore, it helps to deliver a feasible business case and also energy and cost savings for the customers. They additionally give the neighborhood the decision about the source and supply of generating electricity [7].

Microgrids are small-scale versions of the central electrical energy system. They accomplish explicit neighborhood objectives (e.g., reliability, carbon emission reduction, diversification of energy sources, and cost reduction), set up by the community being served. Similar to the bulk power grid, smart microgrids produce, distribute, and control the flow of electrical energy to customers at the neighborhood level. Smart microgrids are a perfect method to coordinate renewable resources at the community level and take into account client interest in the electrical energy enterprise [7].

To optimize the utilization of renewable energy sources, to enhance consumer participation infrastructure, and to guarantee incorporation with IoT at the community level, the microgrid needs to get smarter. A smart microgrid permits bidirectional flow of electrical energy and communication between electricity providers and consumers on the community level. So, to handle the issues of non-accessibility of individual renewable energy sources, IIoT performs a critical job by observing the energy usage, energy generation, and its integrated form, particularly for the smart microgrid. The expression “microgrid” mirrors another state of mind about planning and constructing smart grids. At the neighborhood level, smart microgrids proficiently and financially incorporate buyers and buildings with electrical energy distribution and production. Smart microgrids provide financial as well as environmental benefits to the customer.

Smart microgrids increase dependability locally through the implementation of an explicit dependability enhancement plan that incorporates the excess distribution, intelligent switches, energy production, energy storage, automation, and other related intelligent technologies [7]. Neighborhood electricity production and storage permit segments of the grid and significant services to work autonomously on the big grid whenever essential and therefore remove blackouts. Technologies such as intelligent switches and sensors automatically repair the instability of power, not at all like the present-day electricity systems where switches must be reset manually in the occurrence of an electricity outage. With the help of redundant sources, electricity keeps on flowing even if the storms, ice, or squirrels do any interruptions in the power system. Microgrids also back up the bigger grid when energy demands and expense are most elevated by providing electricity auxiliary facilities [7]. Buyers and businesses in the US pay around \$150 billion per year in expenses because of the outages of power. The dependability of smart microgrids considerably lessens these expenses. It enables buyers to secure energy in real time that again brings down expense at the same time as utilizing neighborhood production to evade peak energy expenses. Furthermore, the smart microgrid infrastructure often incorporates outsider finance. Also, the futuristic upgrade plan for decreasing infrastructure enhancement expenses are mainly paid by ratepayers. Likewise, smart microgrids reduce the cost of energy transmission as compared to traditional grid systems [7].



Buyers and businesses can provide profitable services to the grid as an end result of expenses from the serving utility or autonomous system operator. Smart microgrids likewise set the platform for extra customer earnings from disseminating energy production, plug-in electric vehicles, and carbon credits [7]. This increases fresh business opportunity for stakeholders. Japan and Denmark are leaders in executing the microgrid approach. Recently, Japan's Energy Agency, NEDO, joined with the state of New Mexico to co-fund and create microgrid projects for a number of communities [7].

One of the main advantages of smart microgrids is that they are effectively strategically situated (unlike the centralized grids locations) to fulfill the known and unknown requirements of the future. They permit local communities and commercial campuses to expand the overall electrical energy delivery rapidly and economically through moderately small neighborhood generators, solar cells, wind turbines, etc. This eliminates the waiting for power companies to set up a centralized power plant that is expensive and takes much longer time to start working. The energy management technology of smart microgrids empowers plug-in hybrid vehicles to be connected to the electrical energy system as smart energy storage assets [7].

Another important advantage of a smart microgrid is its capability to utilize neighborhood production and subsequent "waste" heat to uproot coal-fired production. A neighborhood power generator can be renewable or natural gas-fueled. Also, the smart microgrid can recycle the energy generated during electrical energy production for heating buildings, hot water, sterilization, cooling, and even refrigeration. Smart microgrids additionally make it conceivable to take full advantage of clean, renewable energy since they have the adaptability required to utilize an extensive range of energy sources including solar and wind. A smart microgrid empowers customers to meet most of their requirements of electrical energy by producing their own energy, regardless of whether it is through sources like wind, solar, geothermal, microturbines, etc. This would also help to lessen the utilization of fossil fuels and reduce greenhouse gas emissions [7].

### **10.6.2.1 Technologies Used in Smart Microgrid**

There are several emerging technologies available to the smart microgrid construction and operation. At home, we can have smart meters that permit two-way exchange of costing data, utilization data, and electrical energy. There are programmable smart appliances, intelligent gadgets, and user-friendly home energy control systems that enable consumers to connect with the smart microgrid to automatically control each aspect of home energy utilization. Energy efficacy enhancements through further automation assist customers utilize less energy and also reduce monthly electricity bills [7]. At work, the advanced energy control systems help to make commercial buildings "smart". Latest warming and air-conditioning technologies that regulate the building ventilation rates automatically and in real time based on air quality, habitation, the cost of energy, can help improve efficiency. Latest electrical energy

production systems can give energy to singular buildings and deliver energy to the whole grid [7].

Inside the electric energy distribution system, intelligent switches, relays, and sensors that supplant their obsolete and incompetent antecedents can enable the smart microgrid to oversee and distribute energy with greater productivity and dependability. Redundant plans give a backup source of energy when recurring storms, ice, and squirrels disrupt energy supply. Modernized controls that continually check for and even forecast potential instabilities can resolve at least some issues before clients encounter any disturbance in the service [7].

### 10.6.2.2 Project Examples of Smart Microgrids

Here, we present a few examples of smart microgrids based on new technologies.

US Army Forces, Fort Bragg, North Carolina, have developed a smart microgrid. To improve electrical energy supply and dependability while diminishing costs, Fort Bragg in the USA chose to construct one of the world's biggest microgrids. With direction from Honeywell, Fort Bragg incorporated an assortment of distributed production technologies that operate in combination with the military base's utility infrastructure. Covering in excess of 100 square miles, Fort Bragg claims its own electric distribution system that is capable to supervise different productions from a central energy management center. In spite of its size, the different production technologies are completely coordinated with the distribution network, information technology, and communication infrastructure. Because of its smart microgrid distribution system, Fort Bragg have improved its energy provision and dependability and diminished energy expenses [7].

Beach Cities Microgrid Project in San Diego, California, is likewise a smart microgrid. This project has united a portion of the country's greatest names in the power industry to study more about how a smart microgrid in the San Diego region would operate under real-world situations and eventually decrease peak loads by more than 15%. This attempt is driven by San Diego Gas and Electric in partnership with Horizon Energy Group, Advanced Control Systems, Motorola, IBM, Lockheed Martin, Pacific Northwest National Laboratory, and the University of San Diego. Together, they built up a system that includes various distributed production systems, for example, solar power in homes and businesses, biodiesel-fueled generators, distributed energy storage devices, and demand response technologies, for example, smart meters [7].

Perfect Power at Illinois Institute of Technology (IIT) in Chicago is building a smart microgrid. IIT has joined with the Galvin Electricity Initiative and the US Department of Energy (DOE) to build up a perfect power system that is a smart microgrid for the IIT main campus. In collaboration with S&C Electric, Endurant Energy, and ComEd, the university is building an electric energy system of interconnected smart microgrids in a loop configuration with a redundant electrical energy supply. The building of this system is in progress, and it will provide a chance to IIT to wipe out expensive outages, limit energy disturbances, moderate a consistently

increasing demand, and control greenhouse gas emissions. It is anticipated that the smart microgrid will pay for itself as it is constructed over the next five years [7].

## **10.7 IIoT to Combat Challenges of Renewable Energy Sector**

In this section, we elaborate on the inherent challenges and global future of the renewable energy sector.

### ***10.7.1 Challenges of Renewable Energy***

A number of challenges and concerns have already been mentioned in previous sections. Traditionally, a large portion of the concentration in the energy industry has been on diminishing energy consumption when market prices or demand is high, mainly to lessen costs and balance utility load. Such arrangements are intended to reduce the energy deficit. Nevertheless, when energy sources spike, and delivery beyond what the grid can deal with becomes problematic. Quick fluctuations in power load can cause damage to the grid and in addition influence consumers downstream. Regardless of whether a fluctuation goes unnoticed in normal home use, a solitary millisecond of instability can harm computing frameworks or other sensitive devices. Moreover, as we include unusual and variable energy generation to this framework, we have instability on one side from demand and on the other side instability from the expansion of renewable energy.

Up until now, the effect of renewable energy has been relatively undetectable to the framework. However, in certain regions, e.g., Germany, Hawaii, and California, the utilization is increasing at a fast rate. In such situations, it is hard to adjust these three factors: existing generation, the new generation from renewables, and the unpredictability of the demand. To keep up predictable energy distribution, a few utilities have needed to bring fossil fuel generators like coal power plants back online to compensate for a slacker generation. Otherwise, they need to leave windmills sitting idle when the grid is full. To unravel those difficulties, it is required to take a moderate and productive approach to store the excess energy and utilize later when needed [27].

### 10.7.2 *Achieving Grid Stability*

Rather than searching for an answer inside the grid infrastructure itself, there is another methodology discussed in [27]. Imagine a scenario in which it is possible to transform a device (that normally consumes electrical energy) into something that stores energy, and then, we have a way to balance out the grid and the whole energy distribution framework. Now, imagine the usefulness if such a device is embedded in a normal household appliance.

Such innovative ideas have led Steffes Corporation to the development of smart electric water heaters as discussed in [27]. Such moderately cheap devices represent between 20 and 40% of the residential demand or load on energy grids. To make a local and quick reacting storage asset for a distributed system of water heaters, Grid-Interactive Electric Thermal Storage (GETS) framework has been built with the help of Microsoft Partner, Mesh Systems, using Microsoft Azure Platform including Azure IoT Suite and Azure Service Fabric.

Steffes devices are orchestrated by a creative idea called the “Power Tower”, made conceivable by the Azure IoT suite, clarifies TJ Butler, Chief Software Architect at Mesh Systems. The Power Tower is a real-time mirror of every end unit in the cloud and has complicated logic, which facilitates blending and synchronization and utilizes bigger volumes of renewable energy. Microsoft Azure is a cloud platform developed by Microsoft [28].

By exploiting cloud technologies, Steffes devices can interface and control a large number of water heaters and at the same time make a virtual storage asset for utilities. These devices store energy at whatever time it is generated; which may be at night for wind generation or early afternoon for solar, so energy is accessible on demand. With Microsoft Azure, we take an everyday simple device and transform it into an adaptable instrument for overseeing demand, says Murphy of Steffes Corporation. As we get increasingly renewable energy, there is a need to influence load to pursue generation, as opposed to the traditional method for generation following the load. Steffes made water heaters with sensors that empower an organization to monitor up to 150 data points for every unit. In addition to remotely checking the data, the company can control every heater to quickly add or decrease load whenever necessary.

With such approaches as illustrated above, we can reduce the unpredictability and instability that go with renewable energy production resources while at the same time making more prominent the stability and resilience of the electrical grid and distribution framework, says Kelly of Steffes Corporation. This proves that when the normal water heaters meet the Internet of Things, it can transform the energy sector [27].

### ***10.7.3 Global Future of Renewable Energy***

The real-time control empowers to furnish grids with new frequency regulation services that are much more nimble than traditional strategies. To stabilize the grid, utilities companies normally need to throttle these giant machines here and there [27]. Yet, presently they can utilize devices and appliances that are omnipresent in people's houses, which they can aggregate and monitor in real time with second-by-second control. It is considerably more effective than attempting to regulate frequency with large upstream generators. Steffes Corporation has completed 24 separate trials running across over seven time zones.

Hawaii has started to set up the Steffes GETS system in the latest development called Kapolei Lofts that will incorporate 499 rental houses in Western Oahu. Other countries of the world are eagerly watching this venture. In addition to the fact that Hawaii has high daily demand, up to 33% of that demand is provided by unpredictable renewable energy, and they are focused on increasing this figure to 100%. California has focused on 50% and Germany to 45% renewable energy. So if individuals need to comprehend the way the situation is developing, they should examine the developments at Hawaii, California, and Germany.

In addition to furnishing energy companies with accurate control of its grids and distribution networks, Steffes Corporation hopes to cut the upfront expense of water heaters for customers. However, more significantly, it provides opportunities to more people to turn into stakeholders in renewable energy and enhance the global energy environment. This is something that an individual, family, or community can easily do to do their bit on climate change [27]. Consumers can accomplish something at an exceptionally great level to speed up the installation of renewable energy. By utilizing IoT technologies to associate normal consumer devices like water heaters, Steffes Corporation is enabling homeowners to help achieve the vision of sustainability [27]. With this example of IIoT-based water heater project, it is easy to understand the role of IIoT technologies to combat the inherent challenges of renewable energy sources and provision.

## **10.8 Future of IIoT in the Energy Sector**

In this section, we present some future directions by suggesting bonding between buildings and the energy grids, and more discussion on electrical energy generation.

### ***10.8.1 Bond Between Buildings and the Grid***

Our new energy future has many emerging opportunities but also has threats. As DER technologies and strategies, EVs, and IoT proceed to develop further, and the conventional grid develops to a smart grid, the bond between buildings and the grid

will strengthen. Buildings will develop into dynamic partners in the electrical energy sector. Rather than passive loads on the distribution end of a grid that sends electrical energy one way, buildings will also produce electrical energy that would be distributed to neighboring loads or the bigger grid distribution network. Through on-site or EV batteries, buildings will offer crucial energy storage solutions for the advantage of their very own tasks and also for the bigger grid. In addition to producing earnings from conventional building inhabitation, building owners will have the chance to sell electricity and energy services. The job of utilities will probably move from an emphasis on selling electricity to selling grid infrastructure and energy services, in a general sense changing the conventional bond among utilities and their customers of buildings [1].

### ***10.8.2 Market Exchange of Electrical Energy***

The market exchange of electrical energy will likewise change, advancing with the smart grid to a transactive energy approach that empowers a free-market exchange of electrical energy and energy services between an assorted variety of suppliers, including utilities, building owners, and third parties. Our new energy future holds incredible guarantees, and building professionals will become essential partners who would understand the opportunities and recognize and unravel the difficulties on route. Building professionals will be vital in shielding health and sustainability of the constructed environment and the general population it serves. Design, construction, commissioning, and preservation; and tasks and procedures will probably also be changing. There will likewise be extra businesses and whole industry sectors looking to grasp the opportunities.

The technology sector is now occupied with building automation and controls, and renewable production and energy storage. The electricity sector has been functioning at the issues identified with DERs and the smart grid for quite a long while. Data will most certainly be vital to our new energy future, and any company with an enthusiasm for “our” data is now pondering this future. These industries see the probabilities, and they are preparing for the future. Building professionals must be an element of the research, development, and policy changes; the conferences, meetings, and discussions to guarantee the advancement of our new energy future and ready to serve the customers better and support a sustainable world [1].

### ***10.8.3 Decentralization of Energy Generation***

Our new energy future uses decentralized energy generation where smart micro-grid performs a critical role. With the expanded spotlight on pollution-free energy and efficacy as well as the requirement to create the smart grid business system, an increasing number of stakeholders are concentrating on smart microgrids as a practi-

cal and vital way to deal with an upgrade of the grid at the neighborhood level. Smart microgrids increase consumer participation in the energy sector using IoT-based devices [7]—these are like the smart grids.

To optimize the utilization of renewable energy sources, to enhance consumer participation infrastructure, and to guarantee coordination with IoT at the community level, the microgrid needs to get smarter. A smart microgrid permits a bidirectional flow of electrical energy and communication between electricity suppliers and buyers at the community level. So, to handle the issues of non-accessibility of individual renewable energy sources, IIoT performs an essential role by observing the energy usage, energy generation, and its incorporation, particularly for the smart microgrid. Customers and businesses in the USA pay around \$150 billion per year in expenses because of the outages of power. The quality of reliability in smart microgrids can considerably diminish these expenses. It enables buyers to procure energy in real time and altogether bring down expenses at the same time as utilizing neighborhood production to hedge peak electricity expenses. Furthermore, the smart microgrid infrastructure incorporates outsider finance as well as futuristic upgrade plan for decreasing infrastructure enhancement expenses which are mainly paid by ratepayers. Likewise, smart microgrid reduces the cost of energy transmission as compared to traditional grid system [7].

In short, our new energy future includes smart building and smart microgrid as the key elements in the energy sector where IoT plays a crucial role in connecting them. In addition, DERs, energy storage, and EVs also perform an essential role of maintaining grid stability and reliability in the energy sector using IoT.

#### ***10.8.4 Benefits of New Energy Future***

It is essential to highlight that there are numerous potential positive advantages of changes coming to the electrical energy sector and buildings. Expansion of DERs can improve flexibility for buildings and communities, and also the grid. These enhancements offer an incredible guarantee in diminishing carbon emissions and different pollutants to help meet policy objectives and to increase environmental quality. They likewise offer more conceivable outcomes for lessening energy costs. Moreover, with better communication and information exchange through IoT and the smart grid or smart microgrid, there are chances to all the more likely liaison between the design, construction, and operations. This information-rich environment will encourage feedback from a whole integrated design group, and also authorizing and activity groups; and thus giving more chances to keep up design purpose. Our new energy future guarantees to open up new practice areas and open doors for building professionals [1].

## 10.9 Discussion and Conclusion

Expanding requirements for electricity, increased consumption of coal for electricity generation, growth in population, and utilization of renewable energy with its storage requirements are the fundamental reasons behind the changes coming to the electricity sector. Coal contributes to emissions that are destructive to the environment and human health. So, to lessen these emissions, utilization of renewable energy and requirements of its storage are rising. In this context, government agencies are dealing with the advancement of energy infrastructures known as the “smart grid” and “smart microgrid”.

In the present scenario, sensor technology, big data, and data analytics are getting much attention in order to optimize operations, such as efficiently balancing supply and demand as customers connect to a smart microgrid. Usage of smart devices is also increasing; however, their connectivity depends on the speed and reliability of the Internet. Such usage in the industry has resulted in the development of what is called “Industrial Internet of things (IIoT).” Advances in the IIoT help to maximize operational efficiency, optimize business operation, and protect the system. It provides applications like predictive maintenance, remote monitoring, worker safety, and advanced distributed control. So the main objective of this study has been to analyze the IIoT-based renewable energy sector with a view to reducing the use of fossil fuel, increasing the use of cleaner energy resources and better utilization of the energy.

The key contribution of this chapter includes detailed discussion of the concept, history and applications of IIoT; changes coming to the energy sector; introduction of renewable energy and IoT in the energy sector; challenges of renewable energy sector and solutions to the challenges using IIoT; and future of IIoT in the energy industry. This chapter also includes a detailed discussion of smart microgrid which is mainly based on renewable energy and IIoT concept. It determines the role of IoT in smart grid and smart microgrid. Hopefully, the chapter helps us to understand how efficiently the IIoT-based energy system using renewable energy will work for improving the future in terms of better utilization of renewable energy resources as well as limiting the carbon emission. The chapter also includes open research directions in the energy sector and provides several examples of IIoT-based projects in the energy sector.

The overall conclusion of this chapter is that IoT performs a crucial role in the future energy sector for maximizing the operational efficiency, optimizing the business operation, protecting the generation and supply systems, helping with predictive maintenance, worker safety, and advanced distributed control. In order to tackle the problems of non-availability of individual renewable energy sources, IIoT also plays a crucial role by monitoring the energy usage, energy generation, and its integration, especially for the smart microgrid.



## 10.10 Open Research Directions

IIoT in the energy sector is the underlying technology; in this respect, there are many open research directions. There are relatively few published prototypes for the collaboration of renewable and non-renewable energy sources. There are few published prototypes for connecting home apparatuses to the Internet especially for monitoring. There is therefore an urgent need for joining different IoT information frameworks with various sensor input systems in order to increase and promote smart working of connected gadgets. There are very few effortlessly accessible open source simulation tools or the test beds that can allow to empower execution assessment of the IoT-aided SG frameworks [15]. There is a need to comprehend the characteristics of various IoT applications as well as their service requirements in more detail. There is also a need to build practical energy consumption models through the IoT environment, e.g., WSN network [29].

Some of the key challenges of IoT are privacy of data, data analytics, participatory sensing mechanisms, GIS-based visualization, and cloud computing. Moreover, there are some WSN challenges incorporating energy efficacy, architecture, security, protocols, and quality of service [30]. These areas require more detailed research. In addition, there is a need to line up ZEBs with the necessities of the electricity sector [1]. For the future, there is an urgent requirement to develop a methodology for utilizing modern database technologies with considerably more embedded intelligence for even quicker data handling and calculation. This is mainly required in the case of large-scale grid integration with renewable energy sources, especially for solar power plants [22]. These are some of the directions where future research is required to be conducted.

## References

1. Hayter JS (2018) Building our new energy future. ASHRAE J (Aug 2018). [https://www.ashrae.org/File%20Library/About/Leadership/new\\_energy\\_future\\_web\\_061518.pdf](https://www.ashrae.org/File%20Library/About/Leadership/new_energy_future_web_061518.pdf). Accessed on 20 Nov 2018
2. Khan AZ, Abbasi U (2018) An energy efficient architecture for IoT based automated smart micro-grid. Tehnički vjesnik 25(5):1472–1477 (30 Oct 2018)
3. Prez-Lombard L, Ortiz J, Pout C (2008) A review on buildings energy consumption information. Energy Buildings 40(3):394–398 (1 Jan 2008). <https://doi.org/10.1016/j.enbuild.2007.03.007>
4. Javed F, Arshad N (2009) A penny saved is a penny earned: applying optimization techniques to power management. In: The 16th annual IEEE international conference and workshop on the engineering of computer based systems, pp 128–137, 14 Apr 2009
5. The industrial Internet of Things, inductive automation (2018) <https://inductiveautomation.com/resources/article/what-is-iiot>. Accessed on 18 Nov 2018
6. Katz J, Lee E (2018) Industrial Internet of Things (IIoT) in the energy industry. Industrial Internet Consortium. <https://www.iiconsortium.org/pdf/Energy-TG-flyer-Final-v2.pdf>. Accessed on 19 Nov 2018
7. Kelly J, Warner G, Sim F (2018) What are smart microgrids? Galvin Electricity Initiative, 20 May. <http://www.galvinpower.org/microgrids>. Accessed on 18 Nov 2018

8. Hockett L (2018) Internet of Things. Wikipedia, 22 Dec 2018. [https://en.wikipedia.org/wiki/Internet\\_of\\_things](https://en.wikipedia.org/wiki/Internet_of_things). Accessed on 23 Dec 2018
9. Alavi AS, Rahimian A, Mehran K, Ardestani MJ (2018) An IoT-based data collection platform for situational awareness-centric microgrids. In: 2018 IEEE Canadian conference on electrical & computer engineering (CCECE), pp 1–4, 13 May 2018
10. Kang SE, Pee JS, Song GJ, Jang WJ (2018) A blockchain-based energy trading platform for smart homes in a microgrid. In: 2018 3rd international conference on computer and communication systems (ICCCS), pp 472–476, 27 Apr 2018
11. Roy K, Prabhu SM, Koomar A, Karnataki D, Shankar G (2018) Smart IoT based energy metering system for microgrids with load management algorithm. In: 2018 second international conference on computing methodologies and communication (ICCMC), pp 252–256, 15 Feb 2018
12. Aagri KD, Bisht A (2018) Export and import of renewable energy by hybrid micro grid via IoT. In: 2018 3rd international conference on Internet of Things: smart innovation and usages (IoT-SIU), pp 1–4, 23 Feb 2018
13. Adhikaree A, Makani H, Yun J (2017) Internet of Things enabled multiagent system for residential DC microgrids. In: Proceedings of the IEEE international conference on electro information technology (EIT), Lincoln, NE, New York, IEEE, pp 100–104, 14–17 May 2017
14. Phung DM, Villefromoy LDM, Ha Q (2017) Management of solar energy in microgrids using IoT-based dependable control. In: 2017 20th international conference on electrical machines and systems (ICEMS), pp 1–6, 11 Aug 2017
15. Saleem Y, Crespi N, Rehmani HM, Copeland R (2017) Internet of Things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. arXiv preprint arXiv: 1704.08977, 28 Apr 2017
16. Collier SE (2015) The emerging enernet: convergence of the smart grid with the Internet of Things. In: Rural electric power conference (REPC), pp 65–68, 19 Apr 2015
17. Deng R, Yang Z, Chow MY, Chen J (2015) A survey on demand response in smart grids: mathematical models and approaches. *IEEE Trans Ind Inform* 11(3):570–582 (June 2015)
18. Temel S, Gungor VC, Kocak T (2014) Routing protocol design guidelines for smart grid environments. *Comput Netw* 60:160–170 (26 Feb 2014)
19. Ma R, Chen HH, Huang YR, Meng W (2013) Smart grid communication: its challenges and opportunities. *IEEE Trans Smart Grid* 4(1):36–46 (Mar 2013)
20. Wang W, Xu Y, Khanna M (2011) A survey on the communication architectures in smart grid. *Comput Netw* 55(15):3604–3629 (27 Oct 2011)
21. Yaacoub E, Abu-Dayya A (2014) Automatic meter reading in the smart grid using contention based random access over the free cellular spectrum. *Comput Netw* 59:171–183 (11 Feb 2014)
22. Adhya S, Saha D, Das A, Jana J, Saha H (2016) An IoT based smart solar photovoltaic remote monitoring and control unit. In: 2016 2nd international conference on control, instrumentation, energy & communication (CIEC), pp 432–436, 28 Jan 2016
23. Woyte A, Richter M, Moser D, Mau S, Reich N, Jahn U (2013) Monitoring of photovoltaic systems: good practices and systematic analysis. In: 28th European photovoltaic solar energy conference, pp 3686–3694, Oct 2013
24. Constantin S, Moldoveanu F, Campeanu R, Baciu I, Grigorescu SM, Carstea B, Voinea V (2006) GPRS based system for atmospheric pollution monitoring and warning. In: 2006 IEEE international conference on automation, quality and testing, robotics, pp 193–198, 25 May 2006
25. Vidas-Bubanja M (2014) Implementation of green ICT for sustainable economic development. In: 2014 37th international convention on information and communication technology, electronics and microelectronics (MIPRO), pp 1592–1597, 26 May 2014
26. Kashyap S (2016) 10 real world applications of Internet of Things (IoT). *Analytics Vidhya*, 26 Aug 2016. <https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/>. Accessed on 19 Nov 2018

27. Murphy K (2016) Solving renewable energy challenges with the Internet of Things. Steffes Corporation, Microsoft report, 25 May 2016. <http://www.mesh-systems.com/sites/default/files/Mesh%20Systems%20-%20Steffes%20Corporation%20IoT%20Story.pdf>. Accessed on 20 Nov 2018
28. Wei Y, Sukumar K, Vecchiola C, Karunamoorthy D, Buyya R (2011) Aneka cloud application platform and its integration with Windows Azure. arXiv preprint arXiv: 1103.2590, 14 Mar 2011
29. Zhu C, Leung MCV, Shu L, Ngai HCE (2015) Green Internet of Things for smart world. *IEEE Access* 3:2151–2162 (3 Nov 2015)
30. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener Comput Syst* 29(7):1645–1660 (1 Sept 2013)

# Chapter 11

## The Internet of Things in Health Care: Transforming the Industry with Technology



Wesley Doorsamy, Babu Sena Paul and Jerry Malapane

**Abstract** The Internet of Things (IoT) paradigm seeks to integrate physical objects, processes, people, hardware and software, into seamlessly functioning ecosystems. A key application context of this paradigm is the healthcare industry which has the growing challenge of providing affordable quality services with strained resources. This chapter has a focus on the IoT paradigm in the context of the healthcare industry; more specifically, a technological emphasis on IoT use cases in the healthcare environment. The chapter discusses the generic architectural IoT-based healthcare systems and focuses on the development and deployment of wearable and unobtrusive sensing technologies. Although the interest in IoT-based innovation in the field of health care is growing, its widespread usage is rightly encumbered by the critical nature of the applications that necessitate proven reliability through rigorous development and testing. In this chapter, we offer an example of an experimental IoT-based healthcare system and also unpack the details of the various challenges with the different components of IoT systems in healthcare scenarios that affect reliability; we also offer technical insight into future developments and opportunities.

**Keywords** IoT · Healthcare · Wearable technology · Unobtrusive sensing · Patient monitoring · Preventative medicine · ECG · ICG · MCG

---

W. Doorsamy (✉) · J. Malapane  
Department of Electrical and Electronic Engineering, University of Johannesburg, Johannesburg,  
South Africa  
e-mail: [wdoorsamy@uj.ac.za](mailto:wdoorsamy@uj.ac.za)

J. Malapane  
e-mail: [216088717@student.uj.ac.za](mailto:216088717@student.uj.ac.za)

B. S. Paul  
Institute for Intelligent Systems, University of Johannesburg, Johannesburg, South Africa  
e-mail: [bspaul@uj.ac.za](mailto:bspaul@uj.ac.za)

## 11.1 Introduction

The concept of Internet of Things (IoT) has evolved over time, since it was first introduced more than two decades ago [1], going beyond basic integration and automation of components, processes and systems. IoT applications have also gone beyond the manufacturing sector and entered various other areas, inter alia transport [2], education [3], agriculture [4], smart city governance [5], etc. There is also growing interest in the application of IoT in health care, due to the ever-present need for ways to improve quality, efficiency and availability, and reduce costs in this sector. Furthermore, the Things-, Internet- and Semantic-oriented visions of the healthcare services ideally position this sector for the exploitation of the IoT paradigm [6].

In the context of IoT in the healthcare industry, this chapter deals with the technological aspects of the application and various use cases. Due to the growing interest in harnessing IoT innovations for application in health care, the technological considerations (relating to wearables, unobtrusive sensing methods, networking and communications and data management) are presented in this chapter. Components and subsystems of IoT systems in health care are also investigated, including presentation of preliminary design, implementation and testing of an experimental IoT system for smart health care. We also analyze the technical challenges relating to such systems. Opportunities for overcoming these challenges are explored and possible solutions are offered.

In the rest of this chapter, we first contextualize IoT applications in the healthcare industry by giving an overview of the technological evolution of this sector. Thereafter, we deal with the technological layers of the healthcare IoT systems and present a generic system architecture focusing on the sensing layer of the architecture in Sects. 11.3 and 11.4. We then provide an example of a low-cost prototype IoT-based healthcare system and give the technological details thereof. Lastly, we discuss the main technological challenges and opportunities with IoT in health care before presenting a brief summary in Sect. 11.7.

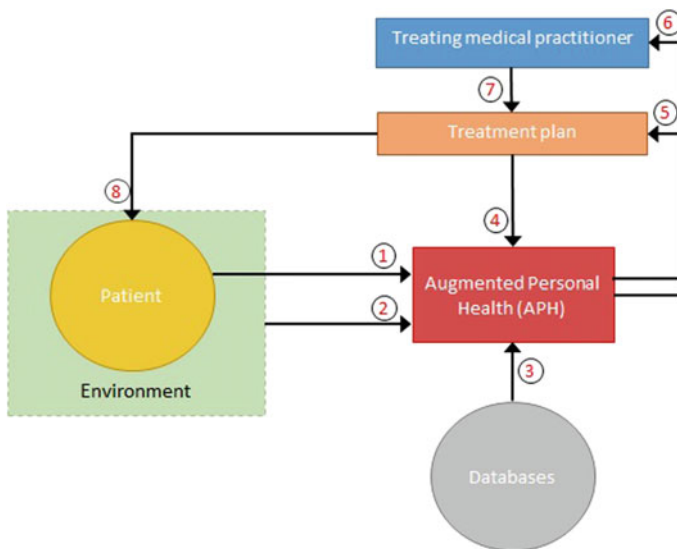
## 11.2 Health Care in the Fourth Industrial Revolution

There are various emerging IoT application domains of health care including healthy living; personal health care; home care; mobile and emergency health care; health-care centers (that include primary, secondary and tertiary health care) and nursing homes for the elderly. Although these domains are directly linked to medical services provided to individuals, the potential availability and seamless sharing of IoT data across these domains are gradually being realized (as highly advantageous) by care providers, treating doctors and healthcare practitioners. They all need to source patients' data to better understand their medical requirements based on history, fitness and well-being.

In the Fourth Industrial Revolution, also known as Industry 4.0 or I4.0, the concept of Augmented Personalized Health (APH) is one that envisages exploitation of IoT and Artificial Intelligence (AI) to promote patient health and well-being through aggregating physical and cyber data (including IoT data, clinical records, clinical practice and medicinal knowledge databases) and converting these data into actionable information. The aim is to assist the unwell individuals with proactively mitigating, preventing or intervening the onset of disease and/or ill-health [7].

The APH vision of future health care is shifting the IoT paradigm, in that, it contemplates a very different approach than current practices. Individuals have the opportunity to receive ongoing care with updated diagnoses and treatment plans without being part of an inpatient program. Figure 11.1 provides an overview of this idea which has already been piloted in the form of mHealth (mobile health care), an application called kHealth [7]. The following are the basic elements and processing of this APH strategy:

- Remote collection of patient-specific data, e.g., patient movement data, condition observations, specific requirements, etc.
- Retrieval of patient-context-specific data such as indoor and outdoor environmental observations, e.g., air quality, temperature, humidity, etc., and situational and lifestyle information.
- Aggregation with supplementary database information consisting of clinical records, regional health data, health practices and other domain-specific knowledge.
- Aggregation of the patient’s treatment plan and medical records.



**Fig. 11.1** Overview of future augmented personal health strategy using IoT

- Semantic annotation of a treatment plan for the purpose of self-monitoring and self-reconciliation tracking; although this is typically not a clinical update to the treatment plan.
- Provision of semantic annotation for physician/medical practitioners for analysis and clinical decision-making updates.
- Medical practitioner's updates to treatment and further courses of action.
- Feedback to patients.

The extent of IoT application varies between different sectors of the healthcare provision. In case of healthcare centers, IoT is gaining more of a foothold in hospitals and specialized healthcare facilities with inpatient programs rather than general treatment centers. General health practitioners' treatment facilities are more likely to utilize data management facilities for streamlining their processes, whereas hospitals and specialized healthcare centers utilize the entire spectrum of IoT-based solutions including wearable, ambient and assistive (to patient and practitioner) technologies. Hence, IoT application differs from segment to segment due to the varying scope of treatment.

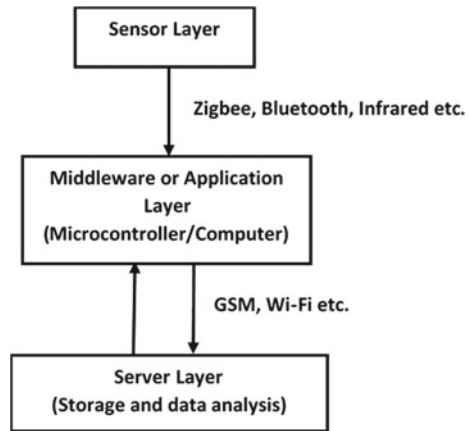
The paradigm shift in the IoT-based health care is most prominent in remote healthcare services as IoT easily affords the possibility of remote medical services provision. Currently, IoT-based outpatient programs enable practitioners to remotely monitor patients (in their home or living environments) and obtain actionable information regarding their course of treatment. Healthy living and personal health care have also entered the mainstream with IoT-enabling self-management, coupled with professional assistance via online databases and communication. In this way, IoT is revolutionizing preventative medicine, early diagnosis of health conditions and control of chronic diseases. Future developments in this sector could potentially extend the provision of medical services to active remote treatment, e.g., automated administering of drugs.

The future of health care is certainly more dynamic with the rapid evolution of sensing, communications and data management technologies available to the industry. Although, the rapid advancement of various technologies deployed as part of an IoT-based healthcare system is clearly evident, and the overall modern system architectures tend to follow a specific trend, as discussed later in the chapter.

### **11.3 Overview of Architecture for IoT-Based Healthcare Systems**

In general, IoT-based healthcare systems consist of a number of key features and sub-systems, which can be described using a generic architecture, as shown in Fig. 11.2. The architecture consists of three main layers viz: the sensor layer, middleware (or application) layer and the server layer. These are briefly discussed below.

**Fig. 11.2** Simplified generic architecture for IoT-based healthcare systems



### 11.3.1 *Sensor Layer*

This consists of different types of transducers and is responsible for collecting data from both the environment and the patients under observation. The sensors can be of different types, e.g., blood sugar level monitoring sensors, skin temperature monitoring sensors, pulse rate sensors, weight sensor, motion detection sensor, etc., as described in the subsequent section.

Data collected by the sensor layer need to be transferred to the middleware layer, also often referred to as the application layer. In practice, technologies deployed in the sensing layer are probably the most rapidly evolving among the different layers and is therefore discussed in some detail in Sect. 11.4.

Communication between the sensor layer and the middleware can be implemented using different protocols and methods such as Zigbee, Infrared, RF, Bluetooth, etc. The choice of communications strategy between these layers depends on the distance between the sensors and the middleware, the available energy and the amount of data required to be transferred.

### 11.3.2 *Application (or Middleware) Layer*

The middleware can consist of a microcontroller or an application that runs on a smartphone or computer. The example presented in the following section utilizes Arduino. The middleware provides an interface between the external world and the sensor layer. Typically, the middleware is not used for processing or storing large amounts of data. A small amount of data may be stored, but this will usually be in the buffer in real time. Additionally, the middleware serves as a gateway to the server layer for exchange of information between the two layers.



### 11.3.3 *Server Layer*

The server layer receives data from the middleware and stores it. The middleware connects to the server layer, typically via GSM and/or Wi-Fi. The server layer is basically a cloud server. It is responsible for storing and processing of required data to obtain meaningful and actionable information. Analysis of certain types of medical data may require domain knowledge experts in the field of medical sciences, and therefore automated processing of data on the server layer may be limited. The example presented in Sect. 11.5 uses ThingSpeak as the server layer.

## 11.4 **Wearables and Unobtrusive Methods for IoT in Health Care**

The technological advances and cost reduction in sensor devices and communications (especially, in the sensor layer of the architecture as briefly overviewed above) are major enablers to the rapid development and deployment of IoT-based healthcare systems. The major trend in the aforementioned sensing layer in IoT health care is a movement toward non-invasive or unobtrusive methods where sensing technologies are enabling more health parameters to be measured using wearables or ambient sensors. Modern inferential methods and algorithms also enable indirect methods of determining health-related parameters. Some of the sensors commonly used for remote monitoring of health provision are in terms of electrocardiogram (ECG), blood pressure, body temperature, blood oxygen levels, pulse rate, electromyography (EMG), movement measurement (accelerometer), galvanic skin response, breathing rate (airflow), electroencephalogram (EEG) and electrodermal activity (EDA), etc. [8].

Recently, there have been some remarkable advancements in medical sensor technologies, particularly for wearable applications. The wearable potentiometric ion sensors are relatively new technology devices consisting of ion detection materials and solid-state electronics for on-body measurements [9]. Due to the simplicity, cost-effectiveness, unobtrusiveness, portability and robustness of such devices, these devices are becoming highly popular in the health sector.

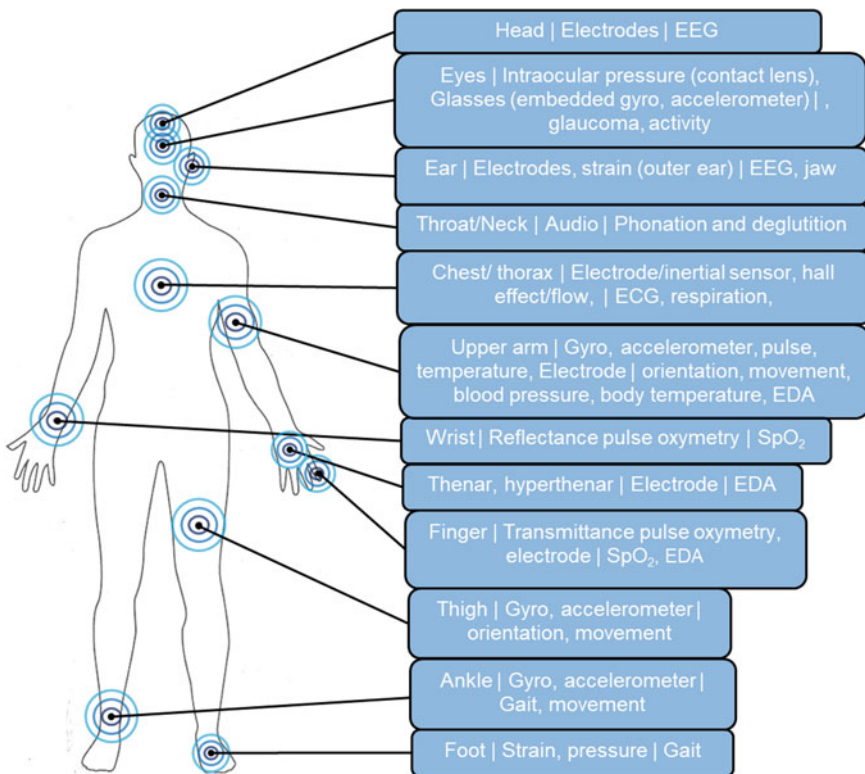
Another sensing platform that has seen recent advancement is conductive polymer composite-based strain sensors used for artificial skin or wearables. The ongoing challenges with this type of platform are fabrication to improve material properties, namely elasticity, anti-corrosion, durability and reliability. Recently, researchers have reported work that addresses these issues through the fabrication of a superhydrophobic strain sensor based on conductive polymer prepared by ultrasonically induced decoration onto a nanofiber surface [10].

Aside from the rapid advancements in fabrication of wearable sensing technology, there has also been progress toward addressing the challenge of reliable energy sources for on-body IoT devices. An example of this progress is presented in [11],

where the development of a wireless implantable sensor prototype with subcutaneous solar energy harvesting is described. This device is essentially aimed at providing a self-powered alternative to batteries for on-body devices, which is intended to be optimally placed between the neck and shoulder of the user.

Wearable technologies are growing rapidly with various types of sensing technologies being developed to assist with the diagnosis of different conditions and/or monitoring of health parameters [12]. These technologies are intended to be worn on several parts of the body. Figure 11.3 provides an overview of the typical areas of the body where wearable technologies are being applied. Some of these new technologies have been commercialized; particularly those used for movement disorders [13], while others are still in development such as the interocular pressure-sensing contact lenses [14].

An emerging sensing strategy in medical applications is ‘sensory substitution’ or ‘sensor modality shifting’ whereby a measured quantity or parameter is used as a means of measuring another parameter [15]. This is particularly useful in medical applications where IoT sensor deployment is constrained.



**Fig. 11.3** Overview of on-body wearable sensing technologies (with associated measurement modalities and applications) in IoT-based health care

There are numerous design constraints associated with IoT sensor deployment in health care. Examples of these constraints include the requirement of unobtrusiveness; limitations on health infrastructure modifications; number and type of body sensors (power, mobility and weight requirements) that can be used, etc. Sensory substitution does provide some assistance with this challenge; however, a management model must be designed in terms of qualitative and quantitative assessment of uncertainty arising from the modality shifting.

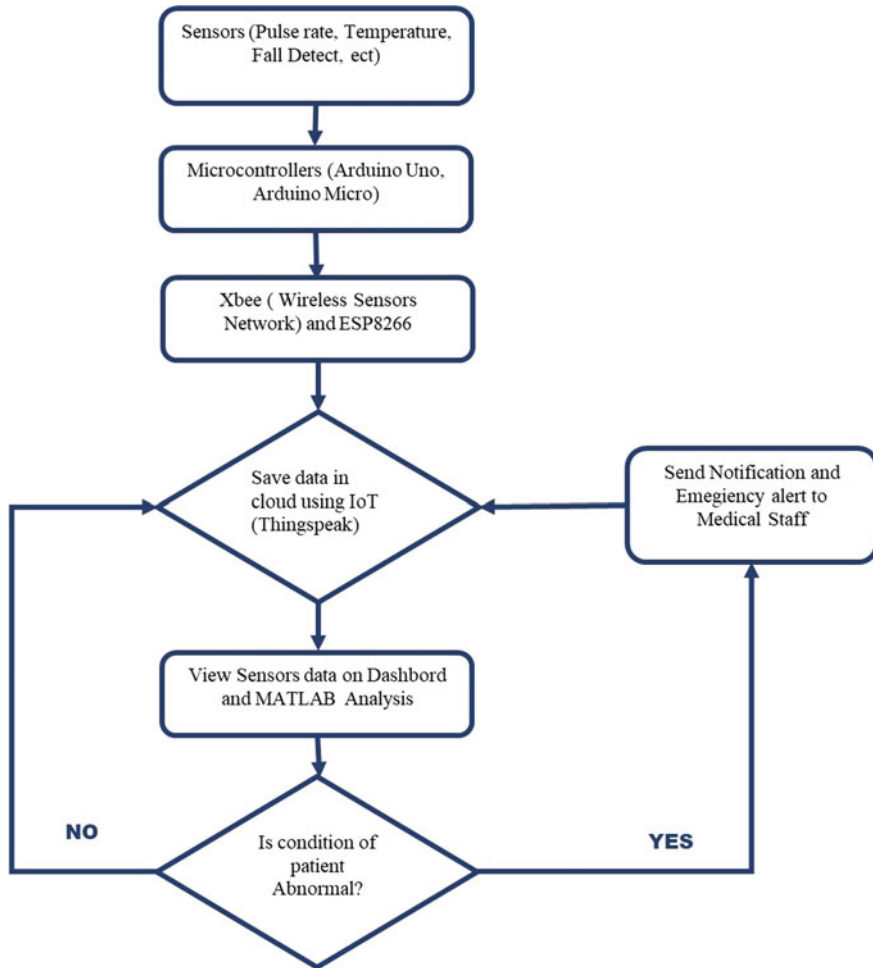
In [16], posture detection, which is necessary for reduction of ulcers or pressure sores arising from limited mobility of patients, is carried out through sensory substitution of the typical methods, e.g., video or pressure sensor array methods, with a combination of thermal and acoustic sensing. Similarly, the method presented in [17] shifts from typical sensing modalities in cardiac monitoring, such as EEG and impedance cardiograph (ICG), to the use of mechano-cardiograph (MCG). This method of MCG performs highly accurate cardiac beat-to-beat detection through recording precordial translational and rotational motions of the chest using miniature inertia sensors, e.g., accelerometric and gyroscopic sensors.

Context awareness is also critical to ensuring the accuracy and reliability of any IoT-based healthcare system. A multitude of sensors is required for providing the context, thereby supplementing the system with information relating to the situation and environment. Additional sensors are therefore required to give context to the 'basic' sensory readings. For example, wearable sensors such as galvanic skin and pulse rate sensors may indicate increased sweating and higher pulse rates, but the supplementary location, ambient temperature and/or movement data of the person give the context of the change in the 'basic' sensor data. The data fusion approach is the key to enabling context awareness and is therefore crucial to the development of reliable and accurate IoT systems in health care. Depending on the data fusion strategy, the model employed may influence the entire IoT system architecture or certain aspects thereof. This approach can help to determine the extent of the sensor network, how the sensor data is collected, at what stage the data is filtered at and how the intelligence and reasoning acts on that data.

## 11.5 Example of an IoT-Based Healthcare System

The presented example of an IoT-based healthcare system is an ongoing developmental project intended to bring together both wearable and ambient sensing concepts into a single cyber-physical system for applications at home or in healthcare facilities. A basic overview of the system function is given in Fig. 11.4. The system architecture follows the simplified generic architecture previously discussed, in terms of the same three layers viz: sensor, application and server layers.

Frail or critically ill patients with hypertension, diabetes and cardiac and respiratory issues require continuous monitoring which is typically carried out manually by doctors and nurses at regular time intervals [18]. Monitoring systems can be used for continuous observation in these situations but such systems typically employ wired



**Fig. 11.4** Basic flowchart of experimental low-cost monitoring system for IoT-based health care

devices that are attached to the patient’s body, thus limiting physical movement. For example, when a patient needs to use the bathroom, the nurse must detach and reattach such equipment. Furthermore, patient observations are recorded via manual entries which are cumbersome, inefficient and susceptible to errors. Some wireless solutions have been developed but they do not make the information remotely available for monitoring, analysis and record keeping purposes. Additionally, these monitoring systems should also have the capability of automatically detecting abnormal conditions and sending out emergency notifications to personnel or care providers.

The aim of the presented system is to address the aforementioned shortcomings through using both ambient and body sensors—in a wireless node configuration that transmits the measured data to be recorded and accessed via the cloud. The

system also utilizes a cloud-resident algorithm to carry out checks on the parameters and sends out emergency alerts accordingly. The system is divided into two main subsystems:

- Patient’s ambient or room environment—which consists of three sensor nodes viz: a bed sensor node, chair sensor node and a patient room sensor node
- Wearable module—that consists of a temperature sensor and pulse rate sensor.

Figure 11.5 gives an overview of the system architecture. The ambient sensor nodes are used to detect the condition of the patient sleeping on a bed or sitting in a chair and also to check the ambient parameters of the patient’s room, such as room temperature and light and movement within the room. Descriptions of the sensors used in such systems and their functionality are given in Table 11.1.

The wearable subsystem consists of a temperature sensor and pulse rate sensor (as shown in Fig. 11.6). The bed and patient room sensor nodes are given in Figs. 11.7 and 11.8, respectively. Each of the nodes utilize an Arduino microcontroller, with the bed and chair sensor nodes communicating through XBee radio modules to the patient room sensor node. The wearable and ambient subsystems then transmit wirelessly to the cloud via Wi-Fi modules.

The preliminary implementation and testing of the suggested system were carried out using ThingSpeak which is a MATLAB IoT analytics platform/service that

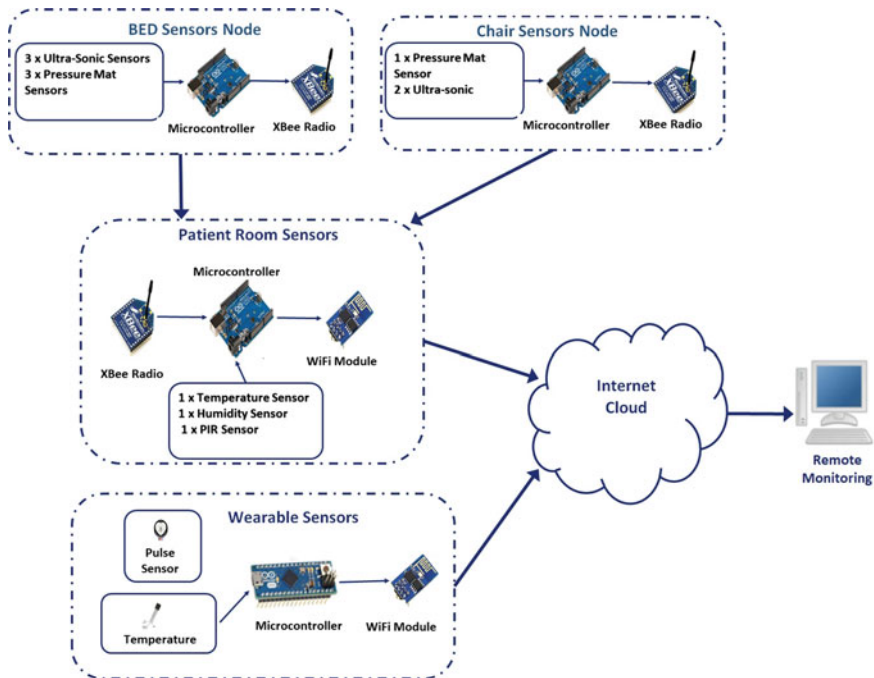



Fig. 11.5 Overall architecture of experimental low-cost monitoring system for IoT-based health care

**Table 11.1** Sensors used in experimental low-cost monitoring system for IoT-based health care

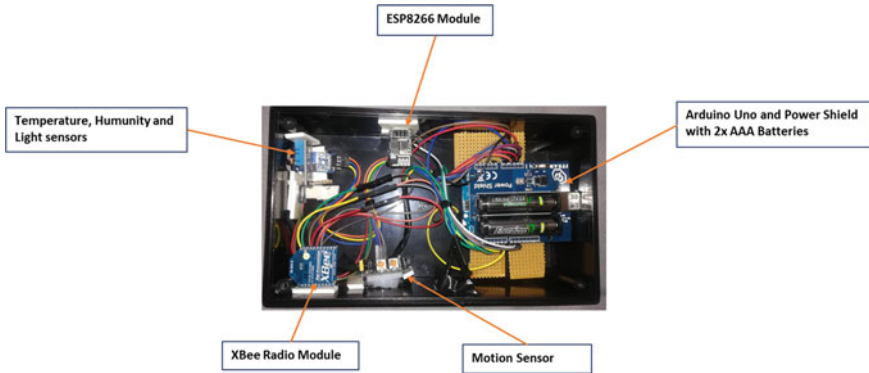
Sensor types	Functionality	Images
Pulse rate sensor	Patient pulse measurement	
Temperature sensor	Skin temperature	
Photo resistor	Ambient light sensing	
PIR motion sensor	Motion detection	
Ultrasonic sensor	Movement detection	
Humidity and temperature sensor	Room temperature and humidity measurement	
Pressure mat sensor	Body pressure detection	
X-band motion sensor	Body movement	

allows a user to aggregate, visualize and analyze live data streams in the cloud. Additionally, the ThingSpeak’s web platform communicates with the Wi-Fi modules that are programmed with the same application programming interface (API) to provide system security.

For testing purposes, the experimental system cloud interface was divided into two channels on the ThingSpeak platform for real-time monitoring and analysis as shown in Fig. 11.9. The two channels being: (1) a wearable sensors channel that provides body temperature and heart rate sensing of the patient; and (2) a patient room channel that provides measurement data of the relevant sensor nodes.

Upon deployment of the cloud interfaces, some basic tests were carried out to check the hardware and software functionality. Figure 11.10 shows the real-time measurements obtained from the wearable subsystem, and Fig. 11.11 shows the





**Fig. 11.8** Patient room sensors node: an experimental low-cost monitoring system for IoT-based health care

Name	Created	Updated
🔒 SMART HEALTHCARE PATIENT ROOM <input type="button" value="Private"/> <input type="button" value="Public"/> <input type="button" value="Settings"/> <input type="button" value="Sharing"/> <input type="button" value="API Keys"/> <input type="button" value="Data Import / Export"/>	2018-05-20	2018-12-23 11:37
🔒 Patient Wearable Sensors Device <input type="button" value="Private"/> <input type="button" value="Public"/> <input type="button" value="Settings"/> <input type="button" value="Sharing"/> <input type="button" value="API Keys"/> <input type="button" value="Data Import / Export"/>	2018-10-17	2018-12-23 09:17

**Fig. 11.9** Cloud channels used for experimental system



**Fig. 11.10** Preliminary results for experimental wearable subsystem function checks using cloud platform



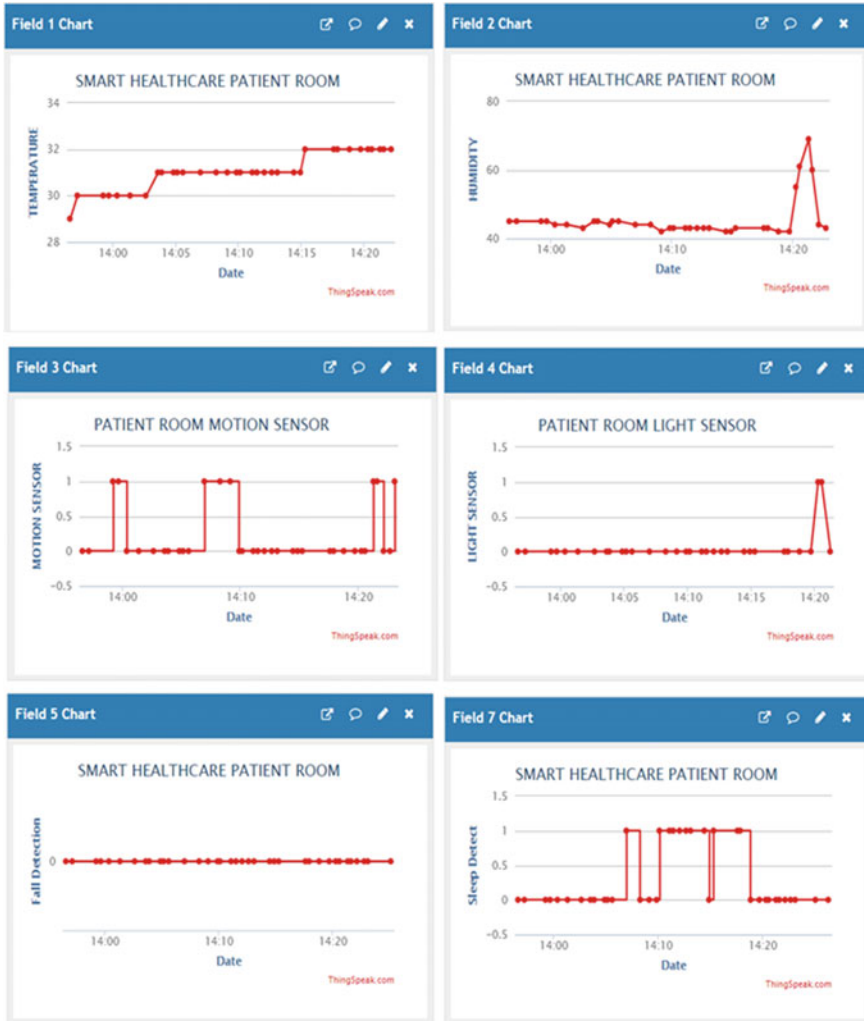


Fig. 11.11 Preliminary results from patient room subsystem function checks using cloud platform

Although the presented results of implementation and testing of the system are developmental, they do demonstrate the potential of IoT deployment in healthcare applications based on the flexibility and range of functionality as well the low-cost of the hardware and software implementation. It should also be highlighted that the architecture of the system also allows for effortless upscaling in terms of the sensor network and data analysis features.

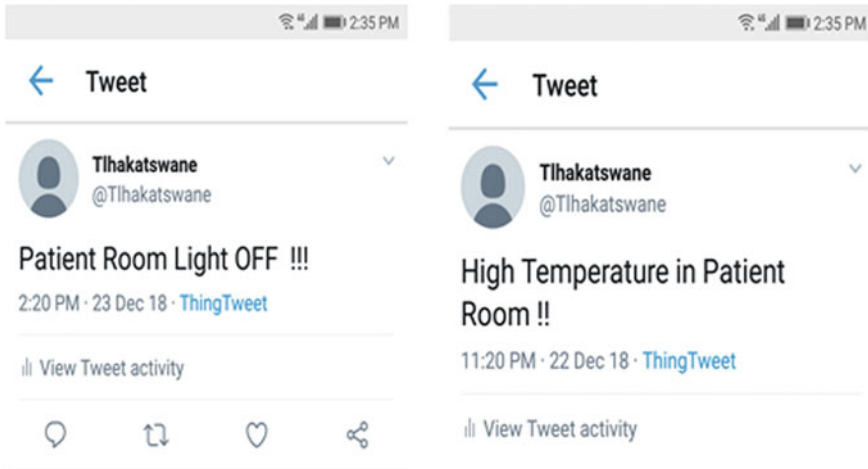


Fig. 11.12 Preliminary results from alert functions using cloud platform

## 11.6 Opportunities and Challenges in IoT-Based Healthcare Systems

Although much work has been conducted in the area of IoT-based health care, with many of these works offering end-to-end solutions, there is no consensus on a consistently acceptable model to be used. Generally, the solutions being suggested are mainly the developmental and generic architectures that tend to feature key components which can be described using the generic models [19].

Our proposed simple model postulates four key elements for an IoT-based healthcare system, namely: (1) sensors and a central node; (2) short-range communications between sensors and central node; (3) long-range communications between the node and the cloud and (4) intelligent and machine learning algorithms, and cloud storage. Most of the solutions being offered place emphasis on sensors—as discussed in this chapter—as this ‘component’ of the generic model is probably the most rapidly advancing. In general, a major challenge with sensors employed in IoT-based health care is the trade-off between reliability and the cost of sensory devices. Many low-cost sensors can provide reasonably accurate measurements; however, these are inappropriate for wearable-based applications. Hence, there is an opportunity for the development of low-cost sensors with suitable robustness and reliability for wearable use, e.g., increased resilience against electromagnetic interference, body motion, etc.

Most systems tend to utilize wireless communication in the form of radio or Bluetooth technologies for short-range communication with central nodes. In long-range communications, LTE can be used but employing a smartphone as a central node presents the limitation of battery life. Dedicated low-power nodes are preferred in these applications. Therefore, effective power management of sensor nodes and communication nodes for wearable and portable ambient sensing applications is

an area of opportunity for further development. In both the short- and long-range communication between components of IoT-based healthcare systems, low latency is an essential design requirement due to the critical nature of the applications. Presently, cloud storage and analytics probably pose the most technical challenges, considering all the related components of the generic model. However, the relevant layers and components also present the areas with the most potential for future development. Some of the major obstacles with cloud computing in IoT-based healthcare systems are summarized as follows [19–21]:

- **Sharing of Resources:** IoT-based healthcare services of the future will share infrastructure and systems. This poses risks such as conflict of interest, compromised security, sharing outside the jurisdiction of law enforcement agencies, etc.
- **Privacy and confidentiality:** A major obstacle refers to ensuring and guaranteeing that patients' data are secure and confidential. Security is a particular concern given that future IoT healthcare services will employ multiple cloud service providers in different countries.
- **Services and standardization:** Due to the complex nature of IoT-based healthcare services, there will undoubtedly be involvement or outsourcing of several services and infrastructure providers. This poses both contract management and legal risks to both the clients and the service providers, particularly in cases where system/service disputes arise. The standardization of these systems for healthcare service provision and surrounding regulations are currently non-existent and will have to be developed over a period of time with the involvement of all stakeholders.
- **Ethics and data management:** The access and usage of patient data by healthcare practitioners and service providers also pose risks to privacy and patients' well-being. Similarly, with the standardization and regulations challenges, ethics and data management policies for healthcare practitioners and service providers, specifically for IoT-based systems, will need to be established.

Currently, work on the data processing and analytics aspect of IoT-based healthcare systems is very limited. Moreover, the intersection of machine learning and domain-specific knowledge in the applications of IoT-based healthcare services is still largely untapped. This is certainly a multidisciplinary area of research and development that is expected to grow in the coming years.

## 11.7 Conclusion

The growing challenge of strained resources in healthcare industry adds to the trilemma of service availability, affordability and quality. The Internet of Things (IoT) paradigm is fast becoming popular in the healthcare industry because it offers technological solutions that can potentially transform the sector. IoT-based healthcare systems are likely to improve the quality of service and assist in the decision-making processes of professionals working in the healthcare sector. With the use of recom-

mender systems embedded in IoT systems for the healthcare sector, more patients can receive quality service in a given period of time with fewer resources.

In this chapter, we began by providing a brief introduction to IoT and its application in different sectors including the healthcare industry. We provided a brief overview on how the Fourth Industrial Revolution is likely to revolutionize the health care sector. Recent advancements in IoT-based healthcare systems indicate the possibility of making high-quality personalized healthcare service both affordable and widely available.

We presented an example of the APH vision, and suggested that, from a technological standpoint, this vision is realizable in the near future. The IoT-based healthcare systems tend to consist of key features which we identified and used to formulate a generic architecture. Technologies relating to the sensing layer of the generic architecture are currently the most rapidly advancing and we therefore focussed on wearables and different unobtrusive methods of sensing along with examples of sensors in development. The preliminary results obtained from the development of an experimental IoT-based healthcare system are presented. This system serves as a basic demonstration of how IoT-based healthcare systems can bring together sensor networks (wearable and ambient sensors), wireless communications and cloud computing to enable low-cost and scalable solutions for continuously monitoring patients and providing medical practitioners with observation information.

This chapter also presented a summary of opportunities and challenges in the implementation of IoT vision in the healthcare industry, specifically with the different technical components of the generic IoT-based healthcare system. While there is still much to be done in all layers of the proposed IoT-based architecture for health care, the major challenges are also found to be in relation to the Cloud/Edge computing paradigms.

## References

1. Ashton K (2009) That 'internet of things' thing. *RFID J* 22(7):97–114
2. Dado M, Janota A, Spalek J, Holečko P, Pirník R, Ambrosch KE (2015) Internet of Things as advanced technology to support mobility and intelligent transport. In: *International Internet of Things summit*. Springer, Cham, pp 99–106
3. Moreira FT, Magalhães A, Ramos F, Vairinhos M (2017) The power of the Internet of Things in education: an overview of current status and potential. In: *Conference on smart learning ecosystems and regional development*. Springer, Cham, pp 51–63
4. Hu S, Wang H, She C, Wang J (2010) AgOnt: ontology for agriculture Internet of Things. In: *International conference on computer and computing technologies in agriculture*. Springer, Berlin, pp 131–137
5. Sebastian A, Sivagurunathan S, Ganeshan VM (2018) IoT challenges in data and citizen-centric smart city governance. In: *Smart cities*. Springer, Cham, pp 127–151
6. Atzori L, Iera A, Morabito G (2010) The Internet of Things: a survey. *Comput Netw* 54(15):2787–2805
7. Sheth A, Jaimini U, Yip HY (2018) How will the Internet of Things enable augmented personalized health? *IEEE Intell Syst* 33(1):89–97

8. Rodrigues JJ, Segundo DBDR, Junqueira HA, Sabino MH, Prince RM, Al-Muhtadi J, De Albuquerque VHC (2018) Enabling technologies for the internet of health things. *IEEE Access* 6:13129–13141
9. Parrilla M, Cuartero M, Crespo GA (2018) Wearable potentiometric ion sensors. *Trends Anal Chem* 110:303–320
10. Wang L, Chen Y, Lin L, Wang H, Huang X, Xue H, Gao J (2019) Highly stretchable, anti-corrosive and wearable strain sensors based on the PDMS/CNTs decorated elastomer nanofiber composite. *Chem Eng J* 362:89–98
11. Wu T, Redouté JM, Yuce MR (2018) A wireless implantable sensor design with subcutaneous energy harvesting for long-term IoT healthcare applications. *IEEE Access* 6:35801–35808
12. Zheng M, Liu PX, Gravina R, Fortino G (2018) An emerging wearable world: new gadgetry produces a rising tide of changes and challenges. *IEEE Syst Man Cybern Mag* 4(4):6–14
13. Jalloul N (2018) Wearable sensors for the monitoring of movement disorders. *Biomed J* 41(4):249–253
14. De Moraes CG, Jasien JV, Simon-Zoula S, Liebmann JM, Ritch R (2016) Visual field change and 24-hour IOP-related profile with a contact lens sensor in treated glaucoma patients. *Ophthalmology* 123(4):744–753
15. Russell L, Goubran R, Kwamena F, Knoefel F (2017) Sensor modality shifting in IoT deployment: measuring non-temperature data using temperature sensors. In: *Proceedings of IEEE international sensors applications symposium*, Glassboro, NJ, USA, Mar 2017, pp 1–6
16. Russell L, Goubran R, Kwamena F (2018) Posture detection using sounds and temperature: LMS-based approach to enable sensory substitution. *IEEE Trans Instrum Meas* 67(7):1543–1554
17. Kaisti M, Tadi MJ, Lahdenoja O, Hurnanen T, Saraste A, Pänkäälä M, Koivisto T (2019) Stand-alone heartbeat detection in multidimensional mechanocardiograms. *IEEE Sens J* 19(1):234–242
18. Ray PP (2014) Home Health Hub Internet of Things (H3 IoT): an architectural framework for monitoring health of elderly people. In: *IEEE international conference on science engineering and management research (ICSEMR)*, pp 1–3
19. Baker SB, Xiang W, Atkinson I (2017) Internet of Things for smart healthcare: technologies, challenges, and opportunities. *IEEE Access* 5:26521–26544
20. Darwish A, Hassanien AE, Elhoseny M, Sangaiah AK, Muhammad K (2017) The impact of the hybrid platform of Internet of Things and cloud computing on healthcare systems: opportunities, challenges, and open problems. *J Ambient Intell Humanized Comput* 1–16
21. Maksimović M, Vujović V (2017) Internet of Things based e-health systems: ideas, expectations and concerns. In: *Handbook of large-scale distributed computing in smart healthcare*. Springer, Cham, pp 241–280

# Chapter 12

## Internet of Things Applications and Use Cases in the Era of Industry 4.0



V. Vijayaraghavan and J. Rian Leevinson

**Abstract** The advent of the Industrial Internet of Things (IIoT) has pioneered a global revolution that is transforming the industrial world. This technological transformation toward a digitalized and connected world improving manufacturing process and production lines with more efficiency, higher capacity, increased worker safety and better return on investment compared to traditional industrial techniques. With the Fourth Industrial Revolution already underway, companies and organizations are swiftly moving toward smart factories, smart workforce, integrated machines and intelligent operations through the use of advanced technologies such as IIoT, cloud computing, cyber-physical systems, artificial intelligence and big data analytics. This chapter explores a variety of IIoT use cases in areas such as manufacturing, automotive, transportation, preventive maintenance production lines, etc. We examine a variety of real-life examples from the industrial sector where companies and organizations have successfully implemented IIoT-based solutions in their factory ecosystems with excellent results. With the global industrial sector advancing toward digitalization and automation, IIoT-based solutions will help to drive digital transformations and thereby create a better future.

**Keywords** IIoT · Industry 4.0 · Manufacturing · Connected industries · Smart factories · Big data · Blockchain

### 12.1 Introduction

The Industrial Internet of Things (IIoT) refers to an interconnected industrial ecosystem in which various machines and objects are embedded with electronic sensors, actuators or other digital devices so that they can be connected and integrated to collect and exchange data. IIoT, also known as Industry 4.0 or I4.0, offers advanced connectivity of physical objects, machines, systems and services, enabling object-

---

V. Vijayaraghavan (✉) · J. Rian Leevinson  
Infosys Limited, Bangalore, India  
e-mail: [Vijayaraghavan\\_V01@infosys.com](mailto:Vijayaraghavan_V01@infosys.com)

J. Rian Leevinson  
e-mail: [rian.leevinson@infosys.com](mailto:rian.leevinson@infosys.com)

© Springer Nature Switzerland AG 2019

Z. Mahmood (ed.), *The Internet of Things in the Industrial Sector*, Computer Communications and Networks, [https://doi.org/10.1007/978-3-030-24892-5\\_12](https://doi.org/10.1007/978-3-030-24892-5_12)

to-object communication and data sharing. IIoT primarily uses IoT paradigms in an industrial environment to build smart factories, optimize production lines, enable customized manufacturing, using connected machines leading to an intelligent workforce.

IoT devices can generate information about an individual entity's behaviors, record it, analyze it and take necessary action. Gartner, a technology consulting firm, estimates that over 6.4 billion connected objects will be in use worldwide this year, in 2018 [1].

The concept of Industry 4.0 (or I4.0) was first introduced at the 'Industrial Internet Consortium (IIC)' which was conducted by AT&T, Cisco, General Electric, IBM and Intel in 2014 [2]. Industry 4.0 which refers to the 'Fourth Industrial Revolution,' is considered the next major technological leap in the industrial world and it is already underway. It is worth noting that the first such technology breakthrough happened in the eighteenth century with the introduction of machines, leading to mechanized production. The introduction and widespread implementations of the concepts of assembly lines and mass production are considered the Second Industrial Revolution and it happened in the early twentieth century. The Third Industrial Revolution was marked by the emergence of digital concepts such as data processing, data storage, computing and Internet in the twentieth century. The Fourth Industrial Revolution is primarily associated with the advent of big data analytics, IIoT, cloud computing, automation, customized productions, smart factories and cyber-physical systems.

Traditional industries rely on mass production and often prefer quantity over quality to generate revenue. In such systems, the products are manufactured in a pre-designed manner and often have limited flexibility and customizability to reduce manufacturing costs. However, with Industry 4.0, individual and customized products can be manufactured at the same cost as that of traditional mass-produced products. They are manufactured by smart factories that have highly optimized and automated production lines.

With this background, this chapter is organized as follows: Chapter 2 introduces the concepts of IIoT and Industry 4.0 while exploring the links between them. Chapter 3 explores the challenges and hurdles faced in the implementation of IIoT systems in industrial settings. Chapter 4 contemplates ways of overcoming the limitations faced by IIoT deployment in industries. Chapter 5 analyzes a number of use cases of IIoT in various industrial sectors such as logistics, warehousing, transportation and manufacturing.

## 12.2 IIoT and Industry 4.0

Although IIoT and Industry 4.0 are closely related topics, in fact almost synonymous, they are not interchangeable and have a lot of fundamental differences. IIoT is a special case of IoT specifically applied to the industrial sector. IIoT is primarily used to connect different machines, systems, networks and vehicles using sensors and gateways. This ensures that machines and vehicles can communicate with each

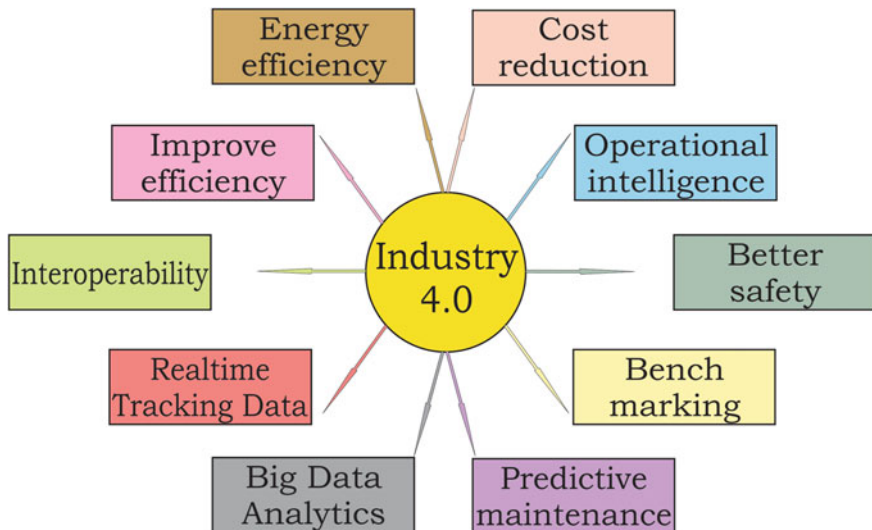


Fig. 12.1 Entities and factors that define Industry 4.0

other and exchange information between them. IIoT solutions can also be integrated with cloud platforms and big data analytics systems to derive deeper insights into the various processes and perform operations more effectively and efficiently [3].

Industry 4.0 refers to an Industrial Revolution that is driven by the efficiency and high level of optimization offered by technological advancements in fields such as IIoT, cloud computing, big data, AI and cyber-physical systems (CPS).

Figure 12.1 depicts various entities and factors that define Industry 4.0. It is predominantly associated with smart factories, intelligent operations, customized products and smart workforce. Compared to traditional factories, modern smart factories have better efficiency, real-time tracking and monitoring of processes, safer operations, better standardization and benchmarking and a high level of integration and interoperability. Moreover, Industry 4.0 can also be considered the coalescence of cyber-physical systems and IIoT [4].

### 12.3 Challenges and Limitations of IIoT

Although IIoT is a revolutionary concept that has the potential to transform the industrial sector, the adoption rate of IIoT technologies is very slow. Many studies and surveys have been conducted to determine the possible factors that could be contributing to the extreme slow and minimal implementation of IIoT-based solutions in Industry 4.0. In a study conducted by IBM in 2015 [5], high investment costs, lack of awareness, complexity, lack of interoperability and lack of flexibility in the



existing IT infrastructure in industries are considered some of the main challenges in the implementation of IIoT.

IIoT solutions are generally expensive with high initial investment costs. This is mainly due to the difficulty in introducing IIoT systems to existing machines and networks. Besides, IIoT also requires the installation of a large number of sensors and supporting infrastructure that are diverse in nature and expensive [6]. The installation and implementation are made even more difficult by outdated machinery, lack of flexibility in the production process and a high degree of manual labor. The situation is further complicated by the fact that industries generally operate with stability as a priority and hence generally refrain from investing in complex technologies like IIoT [7].

Despite the numerous challenges inherent in the implementation of IIoT in conventional industries, it is an investment that is more efficient and effective in the long run. IIoT-based systems will out-perform traditional systems in terms of operating costs, energy efficiency, process optimization, automation and production rate [8]. In the following sub-sections, we elaborate more on the related challenges.

### ***12.3.1 Energy Efficiency***

Although IoT devices are generally small in size, they consume a considerable amount of electricity due to their high processing capabilities. Since full-scale IIoT network implementations may involve thousands of such devices, the efficient management of energy becomes a key challenge. Most IIoT devices run on battery power and are not connected to a direct power source. Moreover, the remote location of these IIoT devices can further complicate the process of maintenance and the process of recharging the batteries.

To overcome these challenges, IIoT technologies have to become more energy efficient and reliable. Ideally, this can be achieved through the use of lightweight algorithms, low-power sensors, efficient processors and optimized algorithms. Using low-power RF transmitters and receivers may also help to increase the battery life of IIoT devices.

### ***12.3.2 Integration and Interoperability***

IIoT systems are generally set up in haste without careful planning or proper network-level architecture. Moreover, IoT devices and sensor manufacturers do not follow any pre-defined manufacturing standards or design protocols. This causes problems in the integration of various IoT devices as different devices tend to be incompatible. This issue becomes more prominent when diverse and complex IoT networks are connected together. This may cause integrity and stability issues, vulnerabilities and incompatibility problems in the IIoT network that can severely hamper operations.

Another challenge faced in the implementation of IIoT solutions is the integration of physical systems and digital networks without considerable data loss or the introduction of vulnerabilities. IoT devices are usually developed as independent solutions and are then integrated with the manufacturing devices [9]. This could lead to a lack of effective connectivity and synchronization between the digital system and the operational system.

Interoperability is another major hurdle in the widespread implementation of IIoT technologies. Integrated IIoT solutions will have the necessity to share data between different systems without issues in synchronization [10]. The issue with interoperability of IIoT devices increases the time taken to implement IIoT solutions in industrial ecosystems substantially and also tends to raise the overall cost of implementation as well. These hurdles have to be addressed by introducing protocols and guidelines in the manufacturing process of IIoT devices to ensure standardization.

### ***12.3.3 Cyber Security***

With the growing number of interconnected IoT devices, networks are increasingly becoming exposed and vulnerable. As devices are interconnected with each other, a breach in any one device in the network can make the entire system exposed to external threats. This is especially the case with IIoT devices as they do not have strict security standards and protocols to govern them. They often tend to have minimal layers of cyber security and use lightweight encryption algorithms and hash tables that are vulnerable to brute-force attacks. These limitations arise primarily due to the low processing power and storage capacities of IoT devices. Since IIoT devices are not manufactured with strict security guidelines, system vulnerabilities and weaknesses are often overlooked.

IIoT devices also need resistance against physical attacks where a device can be opened and accessed physically to gain access to the network. Physical tampering is very difficult to detect and can lead to data loss over time. Therefore, IIoT devices have to be properly secured and should be difficult to access physically to ensure that they are not tampered. As an added layer of security, IIoT networks should use user-based access restrictions and authentication systems to ensure that only authorized personal can access the network [11].

Security concerns are a major challenge in the implementation of IIoT as breaches in security can cause massive damage in the form of confidential data loss, disruption of operations and financial damage. The lack of comprehensive cybersecurity solutions remains one of the main barriers in the implementation of IIoT technologies.

### **12.3.4 Connectivity Issues**

IIoT devices in industries are often placed in remote locations amid active heavy machinery. This not only renders them inaccessible but creates a challenge in connecting the devices together as well. Moreover, devices placed in the vicinity of machinery may experience interference and disruptions in communication. The vulnerability of IoT devices to external interferences is well understood, and adequate shielding is needed. Disruption in the signal can have catastrophic consequences as it could lead to loss of critical information.

Another possible cause of connectivity issue may be due to the large number of devices connected to the IIoT network. Heavy traffic in the network can lead to a decline in the quality of the signal, latency issues and possible data transmission errors and data loss.

## **12.4 Overcoming the Challenges of IIoT**

Although the Fourth Industrial Revolution, with IIoT as one of its key components, is already underway, companies and organizations still face a variety of challenges that prevent them from implementing full-scale IIoT-based solutions to real-life problems. These challenges often tend to hinder the technological advancement of industries across almost all sectors. However, overcoming these challenges offers excellent business opportunities to improve productivity and growth of the respective organization. Most challenges related to the implementation of IIoT can be resolved with monetary investments, awareness, scientific literacy and business initiatives.

Since the implementation of IIoT in existing industries is a very difficult and complicated task, it often tends to de-motivate investors and stakeholders from taking up initiatives. Therefore, it is essential to educate and inform them about the potential benefits of investing in IIoT. Although IIoT-based solutions have high initial investment costs and complexity in integration with existing systems, investors should be persuaded and convinced about the long-term benefits and excellent return on investment associated with them [12].

Standardization of IIoT plays an important role in overcoming the challenges of IIoT. Most IIoT ventures face difficulties in integrating IoT systems with existing systems and also with other IoT networks. This is primarily due to the lack of universally accepted standards and protocols in the design and manufacture of IIoT devices and sensors. Standardization removes most barriers in integration and improves interoperability. Standardization also helps stakeholders analyze the potential profits, hurdles and benefits of IIoT solutions as different networks, applications and systems can be compared easily.

Security is a major issue in IIoT devices. Due to the lack of stringent manufacturing protocols and guidelines, security aspects are often overlooked in IIoT devices. Powerful lightweight encryption and hashing techniques are needed to protect IIoT

networks and devices from cyber-attacks and data thefts. Blockchain and public key asymmetric algorithms are possible solutions that organizations are currently exploring. Moreover, IIoT devices also need to be tamper proof to protect them from physical attacks and data leaching.

Security is an especially serious concern in the industrial paradigm where organizations tend to handle sensitive and critical data such as personal data, financial data, product designs and key organization level plans.

## 12.5 Industrial IoT Use Cases

The Industrial Internet of Things sees potential in a variety of production sectors such as logistics, transportation, manufacturing, energy generation, asset management, smart grids and maintenance. Although a lot of companies have already started implementing IIoT-based intelligent systems in their factories and production lines with immediate positive results, much of the potential for IIoT and advanced AI implementations in the industrial sector remains untapped. This is especially important in the industrial sector, as even small improvements and increase in efficiency can lead to a massive increase in profits and operational savings.

The growth of Industry 4.0 will rest on important key enablers, catalysts and supporting conditions. The key factors among these are continued dynamic innovation, an effective cyber security regime, supporting IT infrastructure and the right talent, skills and expertise. IIoT opens the doors to a variety of benefits for the industrial economy including individual machine optimization, which leads to better performance, lower costs and higher reliability. An optimized machine is one that is operating at peak performance and minimizes operating and maintenance costs. Intelligent networks enable optimization across interconnected machines. Some companies have been early adopters, realizing benefits and overcoming challenges related to capturing and manipulating of data streams. Historically, many of these efforts have centered on the digitally controlled systems of industrial assets with performance scope that is narrow and compartmentalized relative to what is now becoming possible. Given the size of the asset base involved, broader integration of systems and sub-systems at the product level through intelligent devices is expected as the cost of handling and processing data declines.

IIoT has already been successfully implemented in a wide range of industries. IIoT ecosystems are rapidly transforming the industrial paradigm into a smarter one. This has led to revolutionary improvements in the concepts of smart factories, automated warehouses, connected workforce, predictive maintenance, condition monitoring, asset management and quality management. These use cases and their enactment in various industrial sectors are explored in the following sections.

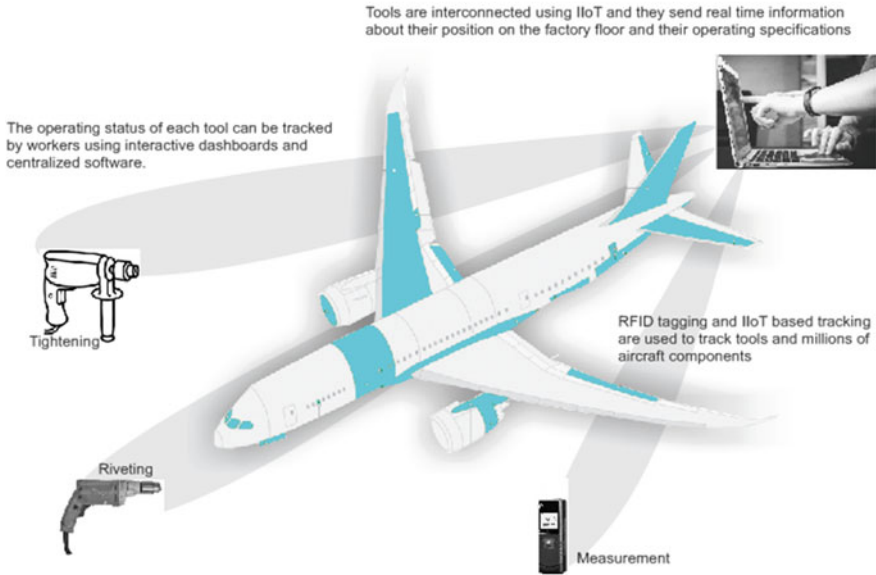
### ***12.5.1 Smart Factories***

Traditional factories lack interconnection between various systems and machines. This renders real-time management of operations difficult and tedious. Smart factories use IoT, cloud computing and big data analytics to integrate various sectors and departments in the factory into a centralized system [13]. IoT-enabled objects that are connected with each other will enable workers to remotely manage the factory units and take advantage of process automation and optimization. By connecting existing assets and equipment across global locations, manufacturers are able to generate live performance data without disrupting production. Connected smart factories provide dashboards to workers that aggregate performance data to provide a holistic view of equipment efficiency, operational statuses and key performance indicators. This enables manufacturers to assess the overall performance of various factories, in real time, by comparing the production performance and working efficiency of machines in the respective factories. With this information, a business can gain insights into the various factors that are contributing to performance variation among factories, and the performance of these factories can be optimized accordingly. Smart factories are the epitome of interconnected production lines with machines communicating with each other using IIoT technologies and a decentralized system that enables swift decision making in an autonomous manner.

#### ***Factories of the Future***

Aircraft are complex machines that are made of millions of different parts that have to be assembled and built with utmost precision and perfection. While dealing with such complex challenges, integrating innovative production techniques is essential. Modern techniques such as graphic prototypes, 3D printing, laser projections, connected tools, robotic exoskeletons for assembly, advanced robots, digitization of the shop floor and integrated production are an integral part of the manufacturing process used in modern smart factories. As shown in Fig. 12.2, IoT and RFID tagging are used to track the millions of parts throughout their journey from various different factories and production lines [14]. Moreover, the location and performance of various tools across the factory are also tracked and processed through IoT gateways.

Assembling an aircraft involves thousands of complex procedures that need to be performed carefully. Since it is not possible to micro-manage all the tasks manually, these process steps have to be integrated and centralized. This can be achieved with the help of sensors-based IoT as the working condition, and the status of every tool across the factory can be tracked and monitored. With this data, the assembly process can be optimized by efficiently managing the tools and resources [15].

**Airbus: Factory of the future****Fig. 12.2** Factories of the future**12.5.2 Condition Monitoring**

Condition monitoring is the process of continuously or periodically monitoring the performance of a system to assess its operating condition and quality of output. It is often performed manually and is an extremely labor-intensive process. Besides, the current automated systems in use offer limited insights into the operations of machines due to physical and technical limitations and also have high investment costs. IoT-based sensors can be used to monitor processes and the operations of machines continuously, in real time as and when required. These sensors are connected to a centralized system that monitors the overall functioning of the machines. Any anomalous or undesired behavior can be immediately detected and necessary course of action can be taken. Traditionally, the working condition and key metrics of machines are displayed locally on the human-machine interface and workers have to work in the vicinity of the machines to continuously monitor them. With a centralized system, a single worker can simultaneously monitor the operation of multiple machines from a remote location. This reduces manual labor, saves cost and time, improves the efficiency of the overall process and improves the safety of the workers as they do not have to stand close to the machinery in potentially dangerous environments.

### ***Cycle Time Monitoring of CNC Machines***

Continuously monitoring the condition of computer numerical control (CNC) machines manually is extremely difficult and tedious. Since employees normally check the vibrations of machines at pre-defined intervals, there is a tendency for problems to go undetected. It is also hard to calculate the cycle time of various machines and pinpoint the exact factors that are causing machines to underperform and affect production [16]. Moreover, there are limitations to the extent to which a CNC machine's processes can be monitored and assessed manually.

To improve the monitoring processes, IoT-based sensors can be connected to the CNC machines to assess their working conditions and monitor key parameters such as vibration, noise, leakages and precision. Any deviations from normal expected behavior are immediately detected and resolved before any breakdown occurs. This reduces unexpected machine downtimes and increases the quality of the final finished outputs and products. It also improves work conditions and safety aspects of the workers as they can monitor the CNC systems from remote locations using handheld smart devices.

### ***Condition Monitoring of Cooling Systems***

Industrial cooling systems work by circulating cooling fluids through the system; the fluids carry the heat away to a heat sink. If the flow in the cooling systems is blocked, the fluid will not be able to transfer heat efficiently and it could potentially cause the temperature of the system to increase. Blockages in the flow of the fluid can also affect the fluid pump and could cause pump failure. Such unforeseen system downtimes can be catastrophic and can lead to massive delays and inconveniences.

To improve the monitoring processes, IIoT-based flow sensors and temperature sensors can be located at strategic points throughout the system to monitor it from remote locations. The flow sensors monitor the rates of flow of the coolants through the system. A considerable decrease in the rate of flow of the coolant can indicate a potential block in the system. The specific region with the constriction in flow can be identified and diagnosed by determining the location of the sensors that detected the issue. By continuously monitoring the status of the cooling system, problems can be proactively detected and necessary action can be taken before system failure [17].

### ***12.5.3 Predictive Maintenance***

Predictive maintenance is the process of anticipating potential failures in the system and scheduling appropriate maintenance before the breakdown occurs. Predictive maintenance can be considered a form of preventive maintenance as the system is, ideally, not allowed to fail and the issues are appropriately identified and addressed before the actual breakdown occurs. In predictive maintenance, various risk factors are assessed, monitored and analyzed to predict the occurrence of failures. It is gen-

erally classified into two types based on the method used to detect the signs of failure: statistical predictive maintenance and condition-based predictive maintenance [18].

Statistical predictive maintenance is based on the data that is compiled from various IoT-based sensors. The data is used to develop statistical models and perform predictive analytics to predict and forecast failures before they actually occur. Depending on the quality and quantity of the data, accurate predictions can be made and potential cases of failures can be identified with high levels of precision.

In condition-based predictive maintenance, equipment and processes are continuously monitored and assessed to identify any anomalies and deviations from desired behavior. The data generated by various sensors is transmitted through IoT gateways and is processed to identify possible scenarios of failures [19]. Once these failure cases are identified, appropriate maintenance activities can be scheduled to prevent undesired breakdowns.

By proactively performing predictive maintenance, the cost and resources associated with maintenance activities that are scheduled on a regular basis can be considerably reduced while the system reliability and operating efficiency are increased. The elimination of unwanted maintenance activities helps reduce cost and increase productivity as the system does not have to be frequently shut down to pave way for maintenance.

### ***Predictive Maintenance for Milling Machines and Heat Exchangers***

Spindles in milling machines are prone to breaking during the production process and repairing spindles can be very expensive. It can also lead to unintended breakdowns and ultimately affect the overall production efficiency. Therefore, predicting the exact time and location of the potential failure of spindles can save money and time. By positioning sensors in close proximity to the machines, vibrations, wobbles and oscillations can be detected especially while performing operations like milling and drilling. This system can be used to manage all the milling machines from a remote location, thereby preventing workers from being exposed to hazardous environments.

Deposits in the filters and ducts of heat exchangers can make them clog, thereby disrupting the flow. Moreover, it is extremely difficult to monitor the flow inside heat exchangers in real time. Due to this, accumulation of particles and development of blockages inside heat exchangers can go undetected. Complete blockages can potentially lead to catastrophic failure of the heat exchangers and can cause extended periods of downtime. IoT gateways and sensors can be leveraged to continuously monitor the flow rate and other vital signs in the heat exchangers. Any deviation from expected behavior can be immediately noted and relevant corrective action is taken [16].

### ***Predictive Maintenance in Railways***

Maintenance in railways is an important and difficult task which, when overlooked, can cause downtimes of critical rail lines. Such unexpected downtimes can cause delays and inconvenience for the passengers and considerable financial loss. Trains can be fitted with IoT sensors that detect wear and tear in various components throughout the system. Additionally, vibrations and noise level can also be monitored using



such sensors as they can highlight potential sources of malfunction. The data from these sensors can be transmitted through cloud platforms and displayed in dashboards so that engineers and maintenance workers analyze the data in near real time and take necessary preventive actions. Unexpected breakdowns and downtimes are thereby prevented by performing predictive maintenance.

As depicted in Fig. 12.3, the entire rail network is connected with a series of IoT-based sensors, devices and components. The system also uses integrated signaling systems and route optimizing techniques to ensure efficient scheduling of trains. Image analytics is also used to perform visual inspection and highlight potential problems. Since the data from all the sensors are compiled to produce a consolidated output, the trains can be monitored from remote locations [20].

### IoT-enabled Truck Fleets

Trucks often tend to travel long distances carrying heavy loads in difficult terrains. To obtain optimum performance and prevent unexpected breakdowns of these trucks, it is essential that the trucks are well maintained. Maintaining fleets of trucks is a massive task for operators in the trucking industry. Truck manufacturers have designed platforms to perform predictive and preventive maintenance by continuously monitoring the status and performance of their trucks. The trucks have a series of IoT-based sensors that are connected to the cloud processing and storage to perform real-time analytics.

The high volume of data generated from these sensors help derive deep insights and develop sophisticated data analysis models. This helps fleet operators manage

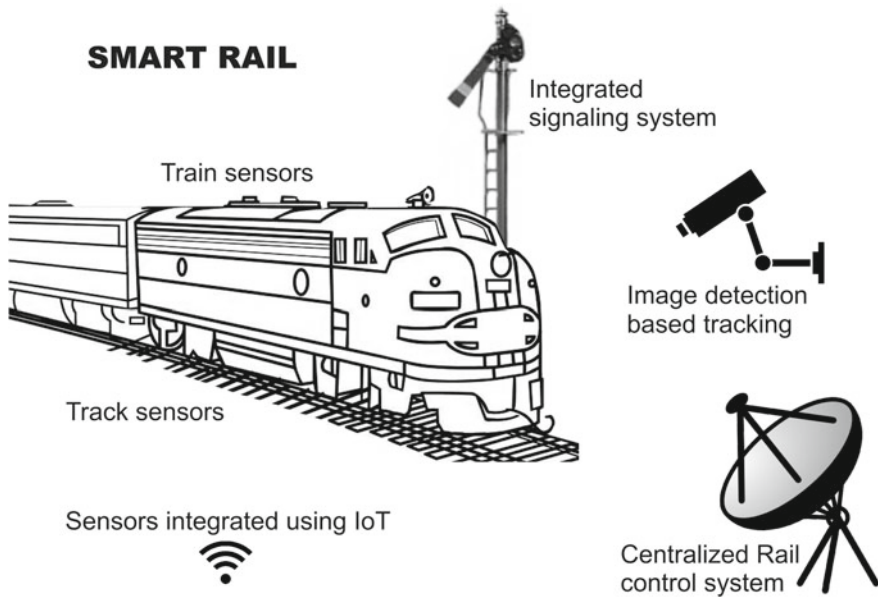


Fig. 12.3 Smart rail

and maintain their entire truck fleet in real time without halting the trucks and performing traditional scheduled maintenance activities [21]. This also leads to efficient micro-management of truck fleets with minimum effort, thereby saving time, energy, labor and resources. Since the performance of the trucks is continuously monitored from a remote location, problems or issues that occur while a truck is on-road are immediately identified and relevant authorities are notified.

#### ***12.5.4 Quality Management***

It is essential to maintain the quality in a production line environment. Products often have to be manufactured with precise requirements and quality standards. The quality and integrity of such products have to be monitored continuously for adherence to quality standards and for optimum output. Conventional techniques generally involve inspecting a few random products for defects and the results are subsequently extrapolated onto the remaining products. Such a randomized sample may or may not reflect the quality of the population and defective products might find their way to the customers.

IoT gateways and connected sensors can be used to continuously monitor the processing units to ensure compliance with quality standards. This enables existing machines to communicate and perform sensor-based monitoring of the products and detect defects and quality breaches in real time.

##### ***Monitoring Lubricants and Filters in Hydraulic Valves***

Hydraulic valves are tested for leakages and manufacturing defects using lubricating oils after production. This test is performed to identifying hidden cracks and faults that may potentially cause failure of the valves. The quality of the lubricants used to test hydraulic valves after production should meet specific preset standards. The oil quality is continuously monitored and maintained to meet the required standards by using IoT sensors. These sensors monitor a variety of parameters that affect the quality of the lubricating oil such as viscosity, oil temperature, presence of contamination and the composition of the oil. Using IoT, the quality standards can also be managed across multiple systems by integrating them into a central system.

Blockages in filters may constrict the flow of hydraulic fluid and could potentially cause catastrophic failure of the system. These blocks are generally difficult to deal with, as the system has to be shut down and the entire section of the hydraulic system has to be checked to identify the location and the cause of the block. By interconnecting the system with IoT-based sensors, the flow through the pipeline system can be monitored in real time. The flow sensors and gauges are continuously monitored to detect anomalies in the flow that could possibly hint towards clogged filters or blockages in the pipeline. The sensors help identify the location of the blockages and necessary action can be taken to clean or repair the filters that may be causing the issue.

### ***Quality Management of the Pressing Process***

Airbag control units are manufactured by mechatronic presses that assemble every component by a mechanical operation called mating. To gain a better understanding of these mating processes and how the process parameters and product quality relate, the process data is extracted from the proprietary press control system. With this data, the force and position of the pressing processes are observed and recorded. This data is used to define a template process which then serves as a reference for each press in the production. This allows a direct evaluation of every single pressing process, based on the raw data. Traditionally, this was only possible with a downstream quality assessment; whereas now, every pressing process is monitored and cross-checked with the template made from the raw historical data. This improves the quality of the products and significantly improves the efficiency of the pressing process.

### ***12.5.5 Assets Tracking***

Assets tracking is a method of tracking, monitoring and locating key physical assets. Industries like Maritime shipping, e-commerce, logistics and transportation rely on assets tracking systems to manage their assets. By tracking assets, organizations can detect inefficiencies through the pipelines, optimize logistical operations, maintain inventory and monitor the working condition of the assets.

The assets and individual entities are tracked using GPS, NFC and RFID tags and the data is transmitted using IoT gateways to a centralized asset management system. Moreover, industries with distributed assets can use IIoT to manage and track their assets [22].

Tracking assets is also important in warehousing to manage stock, monitor inflow and outflow of goods and to track the location of products. Assets management becomes essential especially when the number of assets is large and tracking them using traditional techniques is difficult.

### ***Assets Management and Logistics***

Grocery delivery companies have utilized IIoT technology to dispatch products from their warehouses. They use systems of robots that communicate with each other using IIoT for logistics and warehousing. When an order for a particular product is received, the system automatically assigns a robot to perform the task of fetching the required product and dispatching it for delivery. The robots carry the packages and move through the grid while communicating with each other using the IoT infrastructure. Each of the robot's location is tracked and monitored in real time in a centralized dash board. The robots travel along the grids to retrieve the specific item and ferry them to a drop-off point on the grid to be dispatched [23].

For restocking, the procedure works in reverse where the new stock is classified based on the type of product, and a robot is assigned to place the product in a

specific shelf in the warehouse. This automated system is highly efficient and reliable compared to conventional human-operated warehouses. The system can handle large volumes of traffic and can work for extended periods of time.

### ***Automated Warehouses***

Traditional warehouses consist of racks and shelves that are stacked with various goods. When an order is placed, a warehouse worker receives the specific product's ID and location, and the worker has to manually go to the specific shelf, fetch and dispatch it. Such systems are generally labor-intensive, unsafe, time-consuming and inefficient.

Modern warehouses are automated using technological solutions such as robots, sensors, IoT, digital dashboards and integrated systems. Robots are used to move and store products inside the warehouse, eliminating manual human labor. The robots communicate with each other using IoT technology to optimize the logistical operation and to increase the efficiency of the process. These robots are faster, can carry heavier loads and can work for longer periods of time compared to human counterparts. This system has a high return of investment, increases reliability, improves work quality and leads to a more efficient and safer workplace [24]. Moreover, since robots pack the products into tighter spaces, more products can be stored in the same warehouse.

### ***Connected Tools***

Tracking the location and operation of tools in large factories is a very difficult task. The traditional approach used in the past cannot manage highly sophisticated systems and are not flexible. Manually tracking and documenting each tool's location in the workshop floor is a time- and resource-consuming activity and it is often prone to error and mismanagement.

Modern techniques use integrated systems that consist of tools and machinery that transmit data between each other through IIoT. The tools contain RFID tags and IoT sensors that are used to monitor their location and operating status in real time [25]. RFID is used to track parts when the wireless network is not available or feasible. Information such as the torque, RPM, drill-bit to be used, etc., is displayed on the tool itself, ensuring a smooth and an efficient process. Such innovations not only improve the manufacturing capabilities of smart factories but also reduce cost and improve production efficiency and time.

## ***12.5.6 Fleet Management***

According to a report by the American Trucking Association [26], the US trucking industry accounts for nearly \$700 billion in economic activity. With trucking and transport being a massive industry, it is essential for companies to manage their fleets efficiently. Fleet operators should ideally try to manage their fleets in the most

efficient manner possible to reduce operating costs and to increase profits. Route management, driver performance, vehicle performance and vehicle maintenance are all major factors in the fleet management. Fleet management systems are essential wherever large networks of connected vehicles are used such as the trucking industry, railways, warehouse robots, logistics, etc.

Modern IoT-based systems have a variety of advantages over traditional systems such as optimized logistics, driver performance monitoring for safety, better compliance with environmental laws, efficient route planning and vehicle status tracking for predictive maintenance. Efficient fleet management systems improve the work quality of drivers and reduce driver fatigue by optimizing workload distribution and allotting appropriate workforce for the tasks. Although investing in IoT systems for the entire fleet could be very expensive, the benefits of such an implementation substantially outweigh the downsides of such investments.

### ***Railway Fleet Management System***

Rail transport is reliable, cheap and environment-friendly especially in transporting large volumes of passengers and freight. And with the advent of integrated sensors, predictive analytics, big data and cloud technologies, railways have become more efficient and reliable. An IIoT-based fleet monitoring system introduced in Russia helped in significantly reducing delays and running costs. Sensors placed on the train locomotive and bogies monitor a variety of parameters including engine temperature, closed doors, noise, vibrations in specific coaches, etc. Besides, sensors placed on railway tracks and data from other systems are used to perform predictive maintenance and monitor the location of every individual train in the system [27].

IIoT is also used to micro-manage the railway system to monitor the performance of individual trains and routes. The schedules of trains are planned and changed based on demand in the specific routes. Moreover, the location and speed of the trains are tracked in real time using IoT. This ensures that the trains operate at optimum speeds and loads increasing the efficiency of the overall rail network. By managing the location, movement and operation of every train individually, the efficiency of the overall system is improved and enables the system to operate at maximum load capacity for extended time periods.

### ***IIoT in Garbage Trucks***

Collecting garbage in metropolitan cities is a logistical nightmare as every street and corner throughout the city has to be covered by a limited number of trucks within a specific time period on a daily basis. Such systems need highly optimized routes, sophisticated fleet management systems and careful planning for efficient operation. Modern garbage and waste management companies use IoT sensors on their garbage trucks to track the location of individual trucks in real time. Sensors are also used to measure the amount of garbage collected at various locations. This leads to highly optimized operations and efficient resource management as the routes of trucks can be carefully planned and organized based on demand. Moreover, traffic jams and road blocks can be detected and other trucks can be warned about the hurdles and

can be re-routed accordingly. Since the routes are optimized based on the location of the trucks, it considerably improves the overall efficiency of the fleet management process.

Since the efficient fleet management system of modern garbage companies helps them reduce the cost of their operations, they are able to provide better service to their customers as well. Users can track and monitor the location of garbage trucks in their locality using an interactive mobile app as the data from the truck sensors is relayed in real time using IoT [28].

### ***12.5.7 Worker Safety***

The safety of workers is one of the most important concerns for any industry. According to the International Labor Organization, 2.3 million people worldwide die annually as a result of occupational illnesses and accidents at work. Besides, the report also suggests that over 860,000 non-lethal workplace-related incidences are recorded every day, leading to injuries. The concept of a connected workforce is used to demonstrate how IIoT can be used to improve worker safety and worker well-being, and enable safe work practices. Such a system can monitor a worker's biometrics, exposure levels to nearby hazards and broadcast the information to all nearby workers, thereby avoiding potential mishaps [29]. The reduction in the number of safety-related incidences considerably reduces the insurance costs, the severity of accidents and corporate liability.

A connected workforce is essential in extremely hazardous work environments such as underground mines, construction sites, excavation sites, factories, etc. In dangerous work conditions like these, workers effectively communicating with each other are crucial, and tracking the location and biometrics of workers could save lives.

Such IIoT-based implementations are a major leap in the safety aspects of some of the most dangerous jobs on the planet. It leads to increase in workforce management efficiency, improved resource management, faster operation times and overall worker safety.

#### ***Connected Workforce***

The 'connected worker' is a system that consists of a variety of wearable IoT-based sensors that monitor information about workers and their environments such as toxic gas exposure, breathing, heart rate, posture and motion. A mobile hub system is used to collect and compile information from various sensors. This information can be analyzed in real time to monitor the vital signs of the workers and also to warn them about potentially hazardous situations.

The sensors collect data from a variety of sources including wrist watches, helmets, breathing apparatus, heart rate monitor, activity detection device and motion sensors. The analyzed data is shared on dashboards to the respective plant managers

and incident commanders to inform them about potentially unsafe conditions and dangerous scenarios [30].

In the mining sector, this system can also incorporate a ‘smart tagboard’ functionality that can apply digital technology to know who is present underground at any time to ensure that none of the workers are left behind during emergencies. This is essential as the ability to track the location of individual workers in harsh work environments such as factories and underground mines can drastically reduce the number of safety-related incidences [31].

## 12.6 Conclusion

With the Fourth Industrial Revolution already underway, it is imperative for companies to adopt advanced intelligent systems and methodologies to run their factories. Smart integrated factories are the future of the manufacturing industry with the IIoT paving way for advanced factories that have automated production lines, integrated machines, highly efficient manufacturing cycles, cloud-based big data analytics, complex network of sensors, real-time data analysis, reduced downtimes and increased production capacities. As increasing attention is given to Industry 4.0, intelligent manufacturing is becoming more and more important in the advancement of modern industry and economy. Intelligent manufacturing is considered to be a key future perspective in both research as well as industry, as it provides added value to various products and systems by applying cutting-edge technologies to traditional products in manufacturing and services. Product service systems will continue to replace traditional product types.

While still early in the process, the integration of the industrial world with the Internet and associated technologies could be as transformative as previous historical waves of innovation and change. Advancements in AI and IIoT will pave for a connected industrial world where processes and operations will be integrated, interconnected and optimized for maximum performance and efficiency.

## References

1. Egham (2017) Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent from 2016. <https://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-from-2016>. Accessed Dec 2018
2. Mapifoundation (2015) The Internet of Things: Industrie 4.0 vs the Industrial Internet. <https://mapifoundation.org/economic/2015/7/23/the-internet-of-things-industrie-40-vs-the-industrial-internet>. Accessed Nov 2018
3. Evans PC, Annunziata M (2016) Industrial internet: pushing the boundaries of minds and machines, 26 November 2016
4. Gilchrist A, Nonthaburi B (2016) Industry 4.0: The Industrial Internet of Things. Thailand

5. IBM (2015) “Was kann Industrie 4.0? Und können Sie das auch? Potenzial für die deutsche Industrie.” IBM Corporation, 2015. Accessed Dec 2018
6. Geissbauer R, Schrauf S, Koch V, Kuge S (2014) Industry 4.0—Opportunities and Challenges of the Industrial Internet, PWC—PricewaterhouseCoopers
7. Erol S, Schumacher A, Sihm W (2016) Strategic guidance towards Industry 4.0—a three-stage process model. In: International Conference on Competitive Manufacturing. Vienna
8. Sisinni E, Saifullah A, Han S, Jennehag U, Gidlund M (2018) Industrial internet of things: challenges, opportunities, and directions. *IEEE Trans Ind Inf*
9. Ven R (2018) Top Three Industrial IoT Implementation Challenges, 10 September 2018. <https://dzone.com/articles/3-iiot-industrial-internet-of-things-implementation>. Accessed Nov 2018
10. Bandyopadhyay D, Sen J (2011) Internet of things—applications and challenges in technology and standardization. *Springer Int J Wirel Pers Commun* 58(1):49–69
11. Atamli A, Martin A (2014) Threat-based security analysis for the internet of things. In: IEEE International workshop on secure internet of things (SIoT), pp 35–43
12. Bandyopadhyay D, Sen J (2011) Internet of things: applications and challenges in technology and standardization. *Wirel Pers Commun* 58(1):49–69
13. Zaoini M (2018) Nine Challenges of Industry 4.0. <https://iiot-world.com/connected-industry/nine-challenges-of-industry-4-0/>. Accessed Dec 2018
14. Buntz B (2017) The top 10 Industrial IoT Applications. <https://www.iotworldtoday.com/2017/09/20/top-20-industrial-iiot-applications/>. Accessed Nov 2018
15. Slama D (2016) Airbus introduces the factory of the future, 10 February 2016. <https://blog.bosch-si.com/industry40/airbus-factory-future/>. Accessed Nov 2018
16. Kohler M (2018) Industry 4.0: 10 use cases for software in connected manufacturing. <https://blog.bosch-si.com/industry40/industry-4-0-10-use-cases-for-software-in-connected-manufacturing/>. Accessed Nov 2018
17. Kohler M (2018) Industry 4.0: condition monitoring use cases in detail. <https://blog.bosch-si.com/industry40/industry-4-0-condition-monitoring-use-cases-in-detail/>. Accessed Nov 2018
18. Wang K, Wang Y, Strandhagen JO, Yu T (2016) Advanced manufacturing and automation V, vol 113. WIT Transactions on Engineering Sciences, Boston
19. Ward K (2018) Predictive maintenance. [www.industrialiiotseries.com/2018/07/25/predictive-maintenance/](http://www.industrialiiotseries.com/2018/07/25/predictive-maintenance/). Accessed Nov 2018
20. Lewis K (2017) Just the ticket: Watson IoT helps keep SNCF French National Railway running smoothly. <https://www.ibm.com/blogs/internet-of-things/sncf-iiot-french-railways/>. Accessed Dec 2018
21. Bjorlin C (2018) Volvo Trucks’ IoT-Enabled Fleet Uses SAS to Boost Uptime, 9 November 2018. <https://www.iotworldtoday.com/2018/11/09/volvo-trucks-iiot-enabled-fleet-uses-sas-to-boost-uptime/>. Accessed Dec 2018
22. Nagarajan S (2017) 4 IoT use cases for Industry 4.0. <https://www.ideas2it.com/blogs/industrial-iiot-use-cases/>. Accessed Dec 2018
23. Austin M (2017) This swarm of robots can fill your grocery delivery order in no time at all. <https://www.digitaltrends.com/cool-tech/ocado-robots-grocery-delivery/>. Accessed Jan 2019
24. Knight W (2015) Inside Amazon’s Warehouse, Human-Robot Symbiosis. <https://www.technologyreview.com/s/538601/inside-amazons-warehouse-human-robot-symbiosis/>. Accessed Dec 2018
25. Zhong RY, Xu X, Klotz E, Newman ST (2017) Intelligent manufacturing in the context of Industry 4.0: a review. *Engineering* 3(5):616–630
26. McNally S (2018) [https://www.trucking.org/article/New-Report-Finds-Trucking-Industry-Revenues-Topped-\\$700-Billion](https://www.trucking.org/article/New-Report-Finds-Trucking-Industry-Revenues-Topped-$700-Billion). Accessed Jan 2019
27. Marr B (2017) How Siemens is Using Big Data and IoT to Build the Internet of Train, 30 May 2017. <https://www.forbes.com/sites/bernardmarr/2017/05/30/how-siemens-is-using-big-data-and-iiot-to-build-the-internet-of-trains/>. Accessed Dec 2018
28. Candel E (2017) Cloud computing and IoT in waste management. <https://greenq.gq/>. Accessed Dec 2018



29. Ray B (2018) Industrial IoT: The Essentials of Implementing a Solution, 30 July 2018. <https://www.link-labs.com/blog/industrial-iot>. Accessed Jan 2019
30. Industrial Internet Consortium (2017) <https://www.iiconsortium.org/connected-workforce-safety.htm>. Accessed Dec 2018
31. Hämäläinen P, Takala J, Kiat TB (2017) Global estimates of occupational accidents and work-related illnesses. Accessed Dec 2018

# Chapter 13

## Technology Trade-offs for IIoT Systems and Applications from a Developing Country Perspective: Case of Egypt



Aya Sedky Adly

**Abstract** As technologies and availability of IoT-based services in the industrial sector advance, new demands from users emerge. Every day, we see countless IoT applications appearing on the scene that have a direct impact on society and the public at large. Recently in Egypt, interest in IoT technologies has been emphasized by government ministries and the industrial sector. As a result, the Egyptian government is taking a keen interest to develop IoT-based solutions and attract foreign investment. However, the prevalence of new related technologies is creating confusion and giving rise to more compromises and decisions in industrial systems and applications. These decisions often involve one or more trade-offs. Additionally, there are many inherent challenges that need to be addressed to make IoT deployment more successful and turning these challenges into opportunities with good possibilities to succeed in the future. This chapter aims to address the related concerns and trade-offs for both current and possible future technologies and their deployment in Egypt.

**Keywords** Industry · IoT · IIoT · Industry 4.0 · Trade-offs · Future · Challenges · Automation · Security · Hydro energy · Wind energy · Solar energy · SCADA · Egypt

### 13.1 Introduction

During the 1990s, the term Internet had the implication and vision of a number of computers connected by means of a cable. Even now, for many a youngster, the term Internet or WiFi tends to mean perhaps no more than just Facebook, Instagram, LinkedIn, Twitter, etc.

Currently, the explosion of Internet-based services has resulted in a huge shift in the Internet vision from being technology-driven to being market-driven. This separation between technologies and services has also become the trigger to unlock a new Industrial Revolution. Currently, we are moving swiftly into a world of not only computers and smartphones but also to universally connected smart devices, objects,

---

A. S. Adly (✉)  
Faculty of Computers and Information, Helwan University, Cairo, Egypt  
e-mail: [ayasedky@yahoo.com](mailto:ayasedky@yahoo.com)

and other *things*. It is now the world of Internet of Things (IoT) which is moving from people connectivity to machine connectivity and has the capability of emerging into a new industrial and technological evolution, being dubbed as Industrial IoT (IIoT), also called Industry 4.0 (or I4.0).

Generally, our world is filled with different devices, objects, and things that have different identities, characteristics, and personalities and have the capability of operating in smart environments using intelligent interfaces, communicating with other devices and giving feedback to their users. From one point of view, IoT can be considered as a network of interconnected devices, objects, or *things* that are uniquely addressable using universally accepted standard communication protocols [1]. Another point of view would suggest the combination of information and knowledge obtained from physical actions and vice versa using devices, objects, and other *things* in a new way that did not exist before.

In the global information and services industry, IoT has attracted attention of governments, enterprises, factories, and academia and brought an intelligent new market for the industry community. For a developing country such as Egypt (which has to some extent a limited technology penetration at the national and international level), it is essential to have an efficient infrastructure (to meet IoT-related demands) that is based on present technology advances with capabilities that provide affordable and sustainable solutions. Availability, reliability, interoperability, robustness, integration, standards, and low-cost deployment are currently being considered as the main factors (or requirements) for IoT-based developments and solutions.

The industrial IoT (IIoT) can be useful in many different sectors including the business sector, in particular inventory control, location tracking, shipping tracking, assets tracking, energy conserving as well as customer and suppliers profiling. A great potential lies in controlling, predicting, and automating the related processes and operations, resulting in an effective and efficient value chain with utmost accuracy and profitable benefits.

Considering the substantial importance of the IoT industry in the global economy, academics are also focusing their attention on several issues within a wide range of research topics [2]. Some of these are discussed in the following sections.

The remainder of this chapter is organized as follows. Section 13.2 introduces relevant IoT-based solutions. Section 13.3 briefly discusses the evolution of industrial systems and applications in the context of the IIoT vision. The next section highlights state-of-the-art technologies and trade-offs. In Sect. 13.5, possible future technological developments are articulated; the chapter is then concluded in Sect. 13.6.

## 13.2 IoT Solutions for the Industrial Sector

Demand for services that relies on the Internet is constantly increasing as the needs arise. These services require more efficient human-to-human interactions via communication technologies, as well as human-to-machine interactions (HMI) and machine-

to-machine (M2M) interactions using the interconnected smart devices, artificial intelligence, and ubiquitous computing.

Introduction of radio-frequency identification (RFID) technologies have acted as an initial trigger to extend the IoT vision for communication between the real and the virtual worlds. With RFID, smartphones, sensors, actuators, robotics, and other intelligent technologies, IoT is currently being considered as an important driver to further the cause of ubiquitous and distributed computing. The related technologies enable the IoT to provide services where most of the human senses are somehow reproduced and replaced in the virtual world.

### ***13.2.1 Requirements and Limitations of IIoT Solutions***

The requirements and limitations of the IoT become obvious as soon as a need is felt to integrate diverse devices from various manufacturers with the IoT environment. Before understanding the impact that IoT can have on the way of living, it is important to look at the necessary requirements and limitations.

#### **13.2.1.1 Network Requirements and Limitations**

From an economical perspective, IoT vision is concerned with providing new services through device connectivity, which in turn results in profits and benefits. While from a technical perspective, it is concerned with interconnecting new devices, objects, and other *things* and interrogation mechanisms to develop investable applications. For the Internet to adapt to these connectivity needs, it might have different requirements for the two perspectives.

Currently, in Egypt, nodes on the Internet are usually connected using TCP/IP protocols with the traditional IP addressing and routing capabilities. However, this also requires adapting the TCP/IP to the resources connected with the nodes. This is what is proposed by different protocols such as the 6LoWPAN stack for sensor networks. Another solution is to use new communication suites other than TCP/IP that will then also help with the Future Internet, which is a highly attracting topic for many researches in the hope of achieving better adaptation and deployment of future networks. However, while waiting for the Future Internet to appear in Egypt, the current Internet can prove considerably useful in providing the various IoT-based services. Even though earlier stages of the IoT paradigm were concerned with connecting industrial devices, currently it has moved outside of this arena, to include not only devices but also living *things* such as plants, animals, and even humans.

Another important requirement is to provide multi-networking capabilities. In addition, multicast transport capability would be very beneficial, particularly with high traffic on the roads. Even with fixed access technologies, multi-homing can enable the smart devices to be always-connected.

Today, given the diverse nature and variety of smart objects that can be connected, many communication technologies are directly related to wireless networks where the most promising ones include 4G and 5G cellular systems, wireless sensor networks (WSN), wireless local area networks (WLAN), vehicular ad hoc networks (VANET), and many more [3]. Different wireless technologies that have different characteristics and different capabilities can provide a great aid to the IoT infrastructure specifically in machine-to-machine (M2M) applications [4].

Although wireless networks are essential for the IoT, these have numerous inherent issues and limitations. One of these is that wireless communication normally requires more power than if networks are wired. In Egypt, some of the wireless networks were designed for purposes other than telephony or multimedia applications. Thus, wireless connectivity wastes a huge amount of power when utilizing communication protocols as they are, generally, not optimized for event-driven communication.

Another limitation is that there are no intelligent smart devices that do not operate with an IP address as it produces a heavy overhead requiring extra processing. In fact, instead of using IP addresses, they rely on upstream nodes to provide them with an Internet presence.

### **13.2.1.2 Device Requirements and Limitations**

The vision of IoT is spreading with new capabilities and providing new services to the community, as well as the industrial sector. One important reason is the advances and development of low-cost and yet energy-efficient hardware and development platforms that can combine intelligent processors, microcontrollers with memory, and software components. Accordingly, IoT can be redefined from this point of view as well, as a group of interrelated devices in which sensors, actuators, hardware platforms, and communication technologies are combined to enable humans to communicate with everyday objects [5].

An important component of the IoT structure is the interconnected devices. Thus, knowing their exact state at any point in time is important. The related states may refer to speed, movement, energy consumption, connectivity aspect, location longitude and latitude, and many more. This can also help with what is called context awareness which in turn refers to the ability to detect and manipulate status changes of the devices and objects. If the devices have a good level of intelligence and the IoT hardware development platforms are appropriate, this will simplify matters providing real-time and more precise services for optimal effectiveness.

Thus, hardware development platforms can have a great impact on the overall development process of the IoT as they are responsible for providing prebuilt and ready to program kits that help directly in setting the designers and developers sights on what is required in their projects. Although hardware development platforms have a significant impact, in Egypt, it did not gain much attention due to researchers being often interested on the IoT-based services rather than fine-tuning IoT infrastructure. However, as the number of connected devices, services, and solutions in the IoT

environment is growing exponentially, we are still expecting a similar progress with the IoT hardware developments [6].

Having said the above, sensors which are now more affordable in Egypt and much smaller in size have never been more accessible than they are today. However, for a developing country like Egypt, IoT devices need to operate at extremely low power levels despite the fact that the devices do not often operate continuously. It is also required to integrate processors, communication mechanisms, sensors, memory, and storage. Moreover, IoT devices need to be robust, reliable, and energy-efficient and able to run on batteries for a reasonable duration of time and as and when required. They also need to be able to make use of the renewable energies such as solar radiation for recharging capabilities. Sensors placed in areas where they are exposed to environmental factors need to be resilient and have a reasonable life span. Their design should be such that it simplifies replacing components in a plug and play manner and their quality should be high enough to withstand any environmental situation (rain, heat, dust, etc., in the environment). Knowing the condition of all devices in the network and monitoring their behavior will grant the ability to correct problems and accordingly increase efficiency, reliability, and human trust.

### 13.2.1.3 Application Requirements and Limitations

As devices and networks provide physical bases for IoT, applications are responsible of enabling human–device and device–device interactions in an interoperable, robust, and reliable manner as well as confirming proper data transmission within the desired time space. Usually, device-to-device interactions do not require application interfaces or data visualization; yet software applications are still needed when presenting information to end users in a simple and understandable manner to allow them to interact with the system. It is crucial to develop intelligent and self-governing IoT applications in order to be able to automatically monitor the environment and identify and resolve problems (e.g., with devices and device connectivity) without human mediation.

There are four major IoT features that can have a direct impact on Egyptian industries, viz:

- Automation
- Integration
- Scalability
- Ability to use information from external sources.

These features are now briefly discussed below.

#### **Automation**

IoT automation is far from being simple. It involves the integration of many different processes on many diverse devices (with different communication protocols) with the objective to enhance autonomous operations and significantly reduce human effort and expense.

The manufacturing industry is supported by the need to monitor costs, efficiency, and output to ensure that business activities are reaching their full optimal potential. Enterprise manufacturing intelligence software (EMI) is a software solution that collects and presents manufacturing-related data from a variety of sources in order to provide clear information about the performance of required activities. From this central data store, reporting, analysis, visual summaries, and data synchronization enable a quality and business transformation across the enterprise. Intelligence management software empowers IoT industry to take full control over their data and processes.

Moreover, Industrial IoT must be self-organizing, self-configuring, self-healing, and scalable. It must also consume low energy, have lower cost of operations, be simple to install, and be based on globally accepted standards. It is noteworthy that, with the current automation network standards in Egypt, all this is very hard to achieve.

### **Integration**

Easier-to-deploy technologies, prebuilt integrations, and optimized software and hardware are the main ingredients for a successful IoT vision. However, to ensure the integration of software to deliver the most value, it is important to focus on strategies for bringing all IoT actors who are typically in separate spheres. This will bring huge benefits, as significant improvements in business and financial performance can be realized by linking together the real-time nature of IoT and the Industrial IoT information and processes.

In the case of Egypt, there are even more benefits to achieve. For instance, integrating the data obtained from machines with data from other external sources (e.g., from enterprise resource planning systems (ERP), open databases, and social media) can significantly enhance the added value derived from connecting the machines.

### **Scalability**

As many related activities show, in Egypt, an exponential growth in the number of IoT devices (in relation to realistic applications) will continue at least in the near future. Therefore, scalability (which is the capability of an application or device cluster to be adapted to a wider user base than what was initially or originally intended) is emerging as one of the key requirements for IoT further development.

For this to be realized, it is required to consider a number of challenges. One would be the technical challenge connected with possible geographical distribution over wide areas.

Currently, research on IoT scalability in Egypt may be considered to be still in its infancy, and there exist many IoT frameworks that are targeting industrial communities that still suffer from scalability factors and related requirements.

### **Ability to Use External Information**

The acquisition of information systems can either involve external sourcing or reliance on internal developments and modifications. With today's highly developed IoT industry (in global terms), enterprises tend to acquire information and data from specialized vendors.

The ability to use external information, data, and sources (as additional input is also an important industrial IoT goal) is of utmost importance. Moreover, gathering information from customer relationship management (CRM) or product lifecycle management (PLM) systems further enables valuable insight into the products' or processes' performance. Thus, the ability to use additional information from external sources is an important requisite.

### ***13.2.2 Security and Privacy***

Security and privacy is one of the main network-related issues of serious concern, due to a number of factors, as listed below [7]:

- Lack of feasibility of traditional security schemes involving public-key cryptography for the majority of IoT nodes—this is usually due to cost and high-power consumption requirements.
- The always-connected feature of IoT nodes—these may cause many vulnerabilities, e.g., eavesdropping, software attacks, device cloning, and data stealing [8].
- The large number of IoT nodes and the resulting scale of the IoT network—this may create an unprecedented unacceptably large number of “backdoors” that can be exploited by attackers to carry out physical and network attacks.
- Different service providers—this may mean that the stored personal data in the cloud may be shared with others. Also, the providers deliver their services through “cloud apps” that normally run on a datacenter-scale software platform where the user usually gives access to the service provider. This data sharing with multiple service providers results in new security challenges, which need to be solved mostly on the server side.
- Limitation of energy availability of IoT nodes—this will leave them vulnerable to resource enervation and denial of service (DoS) attacks [8, 9].
- Software and firmware updates—these may become unavoidable as a result of the long lifetime of IoT nodes, which require strong authentication mechanisms to evaluate the authenticity and the integrity of the updates and patches, under tight power consumption budget for IoT nodes.

For the future expansion of the IoT, a credible solution to the above challenges is a fundamental requirement. This is already being reflected in the growth of IoT security spending with a predicted compound annual growth rate close to 25% by 2018 [7].

### ***13.2.3 Feasibility and Effectiveness***

Currently, researchers and industries are reporting a growing interest to boost communication systems' efficiency in order to increase the diffusion of IoT applications



and services with the industry. It has been demonstrated that cooperative networking could be exploited for achieving this goal where cooperation embraces variable protocols, technologies, and algorithms that have the same goal to improve the effectiveness of communication systems.

In order to increase the signal-to-noise ratio (SNR), cooperation techniques can allow multiple sending nodes to transmit data concurrently to the same destination, specifically in the lowest layers of the protocol stack (e.g., virtual multiple input multiple output (VMIMO)). It can benefit from the channel state information (CSI) gained from many nodes while allowing the modulation schemas and transmission power levels to be optimized with the extension of the wireless transmitter coverage.

For the application layer of the architecture stack, network cooperation can be utilized to coordinate services, develop crowd sensing platforms, enforce trust management techniques, manage harvested energy, and optimize intelligent transportation systems (ITSs) [3]. Additionally, cooperation can play an important role in forwarding and routing strategies that are considered with the next hop or the subset of cooperating nodes based on collective feedback mechanism from the rest of the network.

In general, characteristics of the infrastructure of the IoT comprise four particular elements [10] which Egyptian infrastructure for the IoT usually lack. These are reliability, robustness, interoperability, and availability, which are now briefly discussed.

### **Reliability**

This is the ability of a system to continuously function in normal as well as unexpected circumstances. It can also be defined as the probability of performing a specified function without failure for a certain period of time.

Reliability has several dimensions, according to varying perspectives of users. The three components which are determinative for users are: (1) services delivery continuity, (2) system availability and accessibility, and (3) users quality requirement fulfillment.

The reliability of the IoT cannot be evaluated individually as it can only be measured for each service and node separately. Thus, a comprehensive assessment is required that also considers different components of the IoT. Reliability also refers to the expected performance of a system, sources of failure of a system, and their consequences. In such cases, specified mechanisms and specified practical implementations are also required.

### **Robustness**

A system that is able to deal with changes in its operation, without suffering from main damage or loss of its ability to function, may be called robust. It should also be able to absorb security attacks without failing. Devices can even request help in case of failure and have knowledge about their own functioning ability with IoT and related sensors.

The IoT itself should include self-managing, self-monitoring, self-diagnosing, and self-repairing structures. This is to ensure permanent functionality of the system. Engineers and technicians also carry out the responsibility to develop systems that are able to absorb security attacks without failures. This is considered as an important activity as part of the provision of a robust system for the IoT environment.

### **Interoperability**

Interoperability implementation has always been considered important for the IoT paradigm. Interoperability refers to the compatibility of devices, so their communication is correctly and easily possible. It differs from connectivity which means that different devices are linked to each other. Establishment of interoperability is, however, highly challenging.

Separating the IoT technical implementation from its functionality is considered as an effective approach to achieve interoperability. Thus, incorporating a diverse set of technologies into the structure of the IoT allows for the implementation of different solutions to different applications. Moreover, an infrastructure built with heterogeneity in mind is highly capable of implementing newly developed devices and networks as it involves various technologies.

### **Availability**

One of the essential requirements for any technology is the system availability, which can be defined as the proportion of time the system is able for used and the time it takes to recover from a failure. It is very important specifically for the IoT when business and commercial sectors are involved. For example, logistical problems can result from constricted availability which can have a negative effect on supplying and ordering the provision. It can result in cutback in functionality, production stop, sabotage, and reduced transparency. For the end user, a lack of availability may mean that product data is not available or functionality of services is limited including personal consulting services.

Decentralization of the IoT increases its availability. In this case, as the Object Naming Service (ONS) presents only itself, with only one root, the system can suffer from a “single point of failure.” If the one existing root is attacked, e.g., through a denial of service attack causing a breakdown, the whole IoT may be paralyzed. Mostly, roots will be allowed to intercept queries directed to the attacked root and respond to them directly. However, technology in Egypt may not yet be in the position to configure such a mechanism. Furthermore, it would demand that every root has all the available data and this will not be practical.

The system ability to accommodate a large number of subscribers is another requirement of availability. Retrieval of information from the IoT without delays is essential to be guaranteed even if many users are provisioning the same information at the same time.

### 13.3 Evolution of Industrial Systems in the IoT Vision

Various types of IoT-based applications have emerged, and the willingness of enterprises to utilize them is growing rapidly. It has been estimated [11] that the IoT will generate \$14.4 trillion in value with a combination of increased revenues and lower costs and also that it will cause emergence among companies and industries. Evidently, IoT-based services are more optimized toward customers' individualized needs.

In manufacturing, the product life cycles begin with ideas generation and move to order generation through the development and manufacturing of the products and finally distribution to the end consumers. In addition, it ensures satisfactory recycling and all post delivery services [12]. Integrating and connecting all parts of the systems involved in the value chain (to ensure the availability of current data in real time) are considered as the basis for the IoT industry revolution.

In Egypt, deriving the optimal value-added flow at any time in the process is vital. The link between people, objects, and various networks of systems establishes an organized, dynamic, optimized, and value-adding streams among all companies in the supply chain in real time.

Looking back through the ages, we find that humans used mechanization, water, and steam power for manufacturing in the First Industrial Revolution; while mass production took place in the Second Industrial Revolution when there were assembly lines in manufacturing plants with the electricity being a significant input for the operations. The Third industrial Revolution was the era of emerging computerized automation and automated processes with embedded technologies. The inception of cyber-physical systems (CPSs) begins in the present-day Fourth Industrial Revolution, often referred to as Industry 4.0 (or I4.0). In the past, the information and communication technology in the production and manufacturing space was widely adopted. However, with the emergence and adaptation of complicated systems in the present I4.0, it is known as CPSs in the industry or cyber-physical production systems (CPPS) that can obscure the boundaries between the real and the digital worlds [13].

With this background, the IoT role is becoming very noticeable in facilitating access to devices and machines that were previously hidden in well-designed silos in manufacturing systems. This evolution will enable digitized manufacturing systems very rapidly as the IoT is capable of connecting factories to a new range of applications that can run around the production. This could range from sharing the production facility as a service, connecting the factories to the smart grids or enabling more agility and flexibility within the production systems themselves. Accordingly, the production system could be considered as one of the many IoT-based systems, where a smarter, effective, and more efficient production could be achieved.

An IoT-enabled manufacturing system can consist of connected industrial systems that communicate and coordinate information analytics and actions to reduce or eliminate downtime and advance both performance and efficiency. Thus, allowing access to external stakeholders for interacting with an IoT-enabled manufacturing

system is one of the evolutionary steps toward building smart factories. The core elements of the system could be the suppliers of the production tools (such as machines and robots) as well as maintenance and retooling actors, production logistics such as material flow, and supply chain management. It is not required for the manufacturing services and applications to be defined in an intertwined and strongly linked manner to the physical systems, but rather run as services in a shared physical world. As the IoT industrial systems can be adaptive and scalable through software or added functionality, adopting the industrial IoT (IIoT) needs a change that integrates with the overall solutions in the way stakeholders design and augment their industrial systems.

In order to improve the industrial processes, IIoT applications are concerned with utilizing available data, cloud services, business analytics, enterprise mobility, and more. The related technologies involve cloud-based services, embedded technologies, wireless communication, sensor networks, sensing technologies, big data, business analytic software, mobility and identity recognition technologies, wireless networks, and standardization protocols. The IIoT applications usually process data from tens of thousands of edge devices nodes; thus, security is considered a very essential requirement in IoT. In addition, faulty information injected into the system has the potential to be as damaging, as information extracted from the systems through information breach [14].

Considering the above, microelectronics and micromechanical parts merging and deploying the sensing devices, communications ubiquity, rise of the microrobotics and software customization can significantly change the world of manufacturing in Egypt.

### **13.4 Emerging Technologies and Trade-offs**

Recently, new technologies associated with IoT and wearable devices have been considered vital for the main application domains but with different architectures and data models. The high prevalence of new breed of sensors, which have varying precision capabilities and fields of application, has granted the possibility to gather large volumes of data that can be processed and analyzed to provide valuable business insight.

However, the current state of the majority of IoT infrastructures does not permit direct access to the information stored and elaborated by the devices. The only way to access data is through RESTful APIs which are provided by the specific vendors. A RESTful API is an application program interface that uses HTTP requests to GET, PUT, POST, and DELETE data. This particular feature is quite critical as it leaves little space to provide interconnectivity. There are special applications supplied with the smart devices which communicate directly with other physical devices. A developer or end user can access the data solely through the application itself or through the APIs; even the ways in which the vendor applications communicate with the devices cannot be known. In spite of the fact that applications' interfaces introduced

by different vendors are simply accessible, each interface has its own representation and special structure not necessarily complying with accepted standardization and in most cases not even machine-readable [15]. Many different approaches have been suggested to solve the IoT interoperability issues; one of them as reported in [16] was based on opportunistic gateways.

Currently, as a result of the recent advances in computer science and information and communication technologies along with manufacturing sciences, cyber-physical systems (CPSs) are considered as important component of the industrial systems. CPS connects the physical world with the virtual world of information technology and software, which allows utilizing different types of available data, digital communication facilities, and relevant services [17]. However, the adoption of CPS through the IoT, specifically in the industry, has resulted in the creation of vast amounts of data that needs special manipulation and analysis for determining meaningful insight and thus extracting the business value. To solve this problem, big data analytics is a facilitator to overcome the bottlenecks that are created by the data generated by the devices within the IoT [18].

There are many applications of IIoT, where generation of large volumes of data is considered one of the most important outcomes of the IoT paradigm. This data is estimated to be over 40 trillion gigabytes (or 40 yottabytes) by the year 2020 that will need to be appropriately manipulated. Studies expect that, by 2020, there will be nearly 20 billion devices connected to the IoT, where the majority of these will belong to the industrial sector [19].

This large amount of data, referred to as big data, has certain unique characteristics which include high velocity, volume, and variety of information. Additional characteristics of big data are being continuously introduced, e.g., “value” that is now being considered as the most important. Moreover, the identification of patterns in the accumulated data is also essential in order to reach sensible predictive decisions [20]. New technologies such as cloud computing allow the analysis of big data through various data analytic techniques, providing complete access to information and resulting in business intelligence [18].

Accordingly, the cloud environment can be the best place to store and analyze such data. The cloud is not only capable of organizing and analyzing data, it can also provide insight into data and visualize results in real time by combining software, a big data engine, data analytic approach, application platform and a database and even more. However, cloud computing is not fully able to meet every requirement of distributed IoT-based deployments as it provides global centralization [21], especially when there is fast growth in the number of sensing devices, which might be time and power restricted.

A novel trending computing paradigm called fog computing is currently emerging with the ability of extending cloud capabilities, such as storage, computation, and networking, that may enable low latency, low power, and location awareness [22]. The combination between the two technologies (cloud and fog) can also be very beneficial. It should be noted that fog computing is not an alternative to cloud computing, especially for applications related to big data and analytics [23]; rather, it complements and extends the cloud idea.

To increase performance and competitiveness, modern industries are moving toward digitalization. However, digitalization should be further investigated in order to address both existing and future industrial challenges, which are expressed through CPS, IoT, big data, cloud as well as fog computing, and other relevant enabling technologies. Creating agreed-upon standards for connectivity and security is important to ensure a bright future for IoT technologies that can communicate and collaborate. Additionally, another major challenge is utilizing big data analytic techniques to support decisions based on the data generated from the diverse sources of industrial systems, including smart interconnected objects.

Furthermore, data visualization enables users to compare products, see trends, and track generated information in real time. It is the user interface that gives the end users the ability to control their products remotely. Commands can also be sent to products, enabling remote access via the cloud. The management and visualization of information from heterogeneous information sources under the same platform is also one of the main challenges that need to be addressed in digitalized factories.

### 13.5 Emerging Technologies for the Future

Debatably, any entrepreneurial endeavor may need to bet on the future. An entrepreneur can invest time and money, making a novel business model and hoping that in the future, new products and services will become popular and generate a steady flow of revenue for the new venture. Thus, future prediction can be a daunting task with a specific relation between predictions and technological landscape. Determining the cause of success or failure of a particular technology in retrospect is simple, while predicting the future of a particular technology is complicated.

In Egypt, Internet of Things is not yet a reality but rather a prospective vision of a number of combined technologies that can modify the way our societies function. Great interest has been unleashed since the evolution of the IoT, giving rise to many research projects, workshops, and conferences [24].

It was believed as reported in [25] that IoT will have to adapt with over 50,000 billion objects of diverse types and technologies, where interacting with them via the Internet would require standardization to be obligatory. Improving communication between objects and people can be done by developing new media access techniques, communication protocols, and standards. This may be done using different approaches. One approach would require smart wireless identifiable objects and embedded devices encapsulation in Web services. In other cases, there are a number of initiatives including the following: context of Web services and things [26], efficient REST-based communications between embedded systems [27], service-oriented architecture-based Internet interactions [28], that may reveal high potential solutions.

Currently, it is easier to enhance the quality of service aspects (e.g., response time, throughput, resource consumption, availability, and reliability) with the advanced technologies that are coming on board day after day. Additionally, improving man-

agement of complex things structures can be accomplished by discovery and use of knowledge about the availability of services and mechanisms. The large number of things, though, will make their management somehow problematic.

Improving monitoring facilities in tracking objects and people and collecting data about their status and situation for assisting informed decisions may be a solution to this problem. Another way to solve this may be by allowing adaptation, intelligence, autonomous behavior, robustness, and reliability of things [24].

In the following subsections, we illustrate a few possible technologies for the future that extend the IoT paradigm.

### ***13.5.1 IoT and Renewable Energy***

Egypt is a country with plenty of land, sunny weather, and high wind speeds. This makes it an excellent place for renewable energy sources. It even has a natural potential for becoming the world's biggest energy harvesting place as it has the main renewable natural elements to generate energy from wind, sunlight, and water. However, currently, Egypt depends heavily on oil and gas as its main energy supply [29].

Industry is the largest consumer of electricity among all end user sectors. The consumption of electricity worldwide by the industrial sector was 42.1% of total energy produced, according to the International Energy Agency Statistics, for the year 2015 [30]. Recently, this resulted in elevation of interest in the development of industrial energy management around the world, as briefly illustrated below.

- An instant monitoring infrastructure of a renewable energy generation system has been introduced by Kabalci et al. [31]. It is constituted of a wind turbine and solar panel arrays. The monitoring platform is concerned with voltage measurements of the renewable sources. Values are measured and processed by sensing circuits and a microcontroller. The parameter values are then transferred over universal serial bus and saved in a database to inspect the system instantly. Values of each measurement are then periodically analyzed and the saved data managed by the software coded visual interface.
- Goto et al. [32] demonstrated an integrated system that can remotely monitor telecommunications power plants. This system is utilized to maintain and manage more than 200,000 telecommunication power plants with air-conditioning plants that were installed in approximately 8000 telecommunication buildings. The system characteristics include integration, remote monitoring functions, and user interface improvement by utilizing information and communication technology.
- Suzdalenko et al. [33] have studied the issue of non-intrusive load monitoring method for load disaggregation into separate appliances.
- Jiju et al. [34] have demonstrated an online monitoring and control system that is based on android platform for the distributed renewable energy sources. This

approach can use a mobile phone or an android tablet Bluetooth interface as a link for data exchange with the digital hardware.

In many countries, solar photovoltaic (PV) systems are used as main contributors of clean electricity. Electricity generation potential from a photovoltaic system can vary from one technology to another, according to different parameters and locations. On every installation of photovoltaic system, sufficient measures need to be taken to have higher energy potentials. Chances of failure and maintenance problems during the operation of the PV systems are present in spite of the efforts made during the installation or before the installation. These problems are obvious when the PV systems are installed in remote or far away locations. The best approach to cope with these problems may be frequent monitoring. However, frequent monitoring cannot be applicable for a human, as it requires full concentration, attention, and great accuracy to identify a problem or to propose a solution [35]. Accordingly, IoT technology for remote monitoring still needs to be adopted. This would then assist in collecting more detailed data about the objects and provide a variety of new developmental scopes.

For instance, a recent work as reported in [36] was concerned with the development of a wireless-based remote solar monitoring system for renewable energy plants in Malawi in Africa. The aim was to develop a cost-effective data acquisition system that presents remote energy yields and performance measurements. The project provided direct access to generated electric power at the rural site using wireless sensor boards and text message transmission over cellular network. Preliminary experimental results showed that the performance of renewable energy systems in remote rural sites could be assessed effectively at a very reasonable cost.

Among the wider applications of the IoT, researchers have also focused on the solar photovoltaics (PV). In Egypt, the prevalence of solar PV systems would have a considerable scope for implementing IoT systems, which would indirectly give an extensive business for both the IoT service providers and the IoT-based service consumers.

### 13.5.1.1 IoT and Hydro Energy

Hydro power systems, particularly small plants, are the most reliable among potential renewable energy production systems since there are many sources of natural water such as springs, waterfalls, rivers, streams, creeks, and tributaries [37]. A hydropower generation system may be able to produce power that is sufficient to supply a rural community village in Egypt that has small electricity consumption. In addition, this system does not use fossil fuel, and so, it is free from pollutants [29].

If implemented in Egypt, an IoT hydropower system can minimize the investment cost, particularly in relation to maintenance, as IoT connectivity offers a host of development opportunities in control, monitoring, and maintaining remote systems. The system can consist of sensors, such as application-specific integrated circuit (ASIC) microcontroller, and a global system for mobile communication (GSM) module. A water-level sensor to detect the appropriate water level is needed due to seasonal



fluctuating water levels as the unit should not generate power when there is too little water, and accordingly, the turbine would not power up. A water flow sensor is also needed to measure how much water has moved through. A pH sensor is also needed to measure the hydrogen-ion activity in the water in order to maintain the durability of the system over time. The ASIC microcontroller is required to read the inputs from these three sensors and send the information via IoT infrastructure for monitoring purposes. Finally, the GSM module or any telemetry system can be used to feedback the community by monitoring the system [38].

Another scenario for a hydropower generation system with IoT-based data monitoring system may be to do with producing sufficient amount of energy by the rapid flow of water from a collector tank collecting water from the rain and other sources. In this way, the rainwater can also be put to a good use and energy can be produced from this water resource which is renewable. The main water tank which is above the ground level can provide a rapid flow down to the underground mechanism of turbine engine which is connected through pipes. The pipes are responsible for the water flow through the tanks located underground. Each pipe should be mounted with sensors that are calibrated to assist to provide the information of water flow in the pipes. The use of sensors attached to the tanks is mainly for the water-level indication which can restrict or allow the flow of water into the tank when needed. The used water for power generation is never wasted as it can be used several times to make the system more efficient. The whole underground system is usually separately connected to an Arduino-based system which includes the display and the WiFi modem for the data transmission to the IoT server. The Arduino can take care of the mechanism for the sensor calibration in the pipes and the tanks. All the data received can be displayed on an LCD panel. Besides sensors in the pipes and tanks, there are voltage and flow of current sensors attached to detect the power generation accurately in needed terms as per the parameters there. In this way, the entire information can be transferred to the server through IOT, and the amount of energy produced is determined [39].

### 13.5.1.2 IoT and Wind Energy

Although technologies involved in hydro and wind power energy are basically the same, in case of Egypt, potential in wind energy is much greater. To take advantage of the full potential, existing data from wind turbines and farms needs to be analyzed, while additional new data needs to be generated through advanced measuring technologies or communication networks. However, if all the information could be gathered, we would indeed get very different insights on how processes are running. This is the vision of the IoT and cyber-physical systems (CPSs), which is to connect everything through networking to facilitate access, minimize errors, and enhance performance.

Thus, as CPS builds a tight coupling between the digital and physical worlds, the implementation of CPS within the IoT with respect to wind energy or any renewable energy promises a great potential for future renewable energy applications. All processes in wind energy could be controlled and optimized automatically, including

accurate real-time monitoring of wind turbine components and efficient maintenance. Integration into existing energy system and maximization of efficiency, reliability, and adaptability can be supported by implementing CPS in renewable energy sources like wind power. In some countries other than Egypt, some varieties of CPS within IoT already exist in current wind turbine technologies.

Two of the technologies for the above scenarios are as follows: condition monitoring system (CMS) and supervisory control and data acquisition (SCADA). These are now briefly elaborated below.

### **Condition Monitoring System (CMS)**

CMS is a reliable and fast-reacting security engineered system that can operate as control system to detect mechanical and electrical faults in core components of machines and maintain permanent monitoring of the machine conditions. It can also analyze and measure physical parameters such as vibration and temperature [40]. Based on such parameters, the operational mode can be modified in case of suspicious measured data. The integrated sensors can also measure the data in real time.

Fiber Bragg grating (FBG) sensors can feature fast responses and measure temperatures, pressure, and vibrations [41]. These are considered as examples for advanced sensor technology for wind turbine applications. They are suitable for monitoring systems due to their small size. They can also be used for blade supervision in current wind turbine applications and offer high reliability and durability.

Vibration analysis is a common feature of a CMS that is capable of detecting deviation in normal ranges of stress. While CMS sensors collect high frequent data at different locations from vibration sensors of the wind turbine's drivetrain, the other sensors may analyze and measure the characteristics and velocity of the main bearing, generator, and nacelle.

Fourier transformation may be used to convert time history response data into frequency domain in order for damage cases to be predicted earlier, so that wind turbine components' damage may be avoided by statistical algorithms.

The alarm systems may be classified according to the severity and lead times for each of them. Despite the fact that CMS gathers wind turbines data in discrete-time intervals, it can monitor the system state at selected measurement points. Thus, it is desirable to have a CMS that is able to measure and monitor continuous loads of all relevant machine components. Also, moving from reactive to predictive maintenance is necessary for enhancing wind turbines capability in the future. It is noteworthy that the application of CMS within the IoT is substantial in sensitive and expensive machine components like the gearbox [42].

### **Supervisory Control and Data Acquisition (SCADA)**

The most important aspect that affects the operation status and power output is the physical environment of wind turbines. As the wind turbine performance accentuates with the power of wind speed, an incorrect forecast of wind characteristics can result in power deviation. Accordingly, all relevant operating conditions and wind properties should be considered important for operators of wind turbines and farms. Wind

properties may include speed-, direction-, turbulence-, and energy-related information, e.g., vibration level, temperature values, power output, and generator torque [43].

In this context, supervisory control and data acquisition (SCADA) is an accurate and modern sensing technology system which can provide the needed wind turbine data. SCADA systems can transmit and collect various data streams at discrete-time intervals through sensors. Remote controlling of the physical systems can be realized through almost real-time overview that could be obtained via the wind turbine conditions. This information can be available to operators and customers all over the world, as long as it is stored online.

An example would be a monitoring control system that constitutes SCADA which achieves real-time monitoring and control of a hybrid “wind PV battery” for renewable energy system [44]. This system can be used to measure electrical data in real time and then effectively send it to remote monitoring center via the Intranet. It is found from the experimental studies that this system can carry out data acquisition of different remote forms of renewable energy system and real-time supervisory control. Overall, SCADA systems simplify and advance automated remote monitoring in addition to being able to promote wind turbine operation [42].

## 13.6 Conclusion

The Industrial IoT represents a future vision of ubiquitous connectivity of smart objects. Connecting devices, components, sensors, actuators, animals, plants, and humans to the Internet greatly increases the potential range of applications and the flexibility, reliability, usefulness, effectiveness, and scope of the networks. From this perspective, the IoT pushes such capabilities beyond personal devices (e.g., smartphones), embedding them in everyday objects and living environments.

Although there is much ongoing activity in Egypt on the various aspects of the IoT, the convergence of previously separate industry sectors has led to some overlap and confusion. Industrial processes and logistics can highly benefit from the IoT, as it enables ubiquitous sensing of operating conditions, real-time tracking of semi-finished products, detection of events that slow down the process throughput and potential safety issues. The data generated in the production line can be intelligently shared with the quality assurance processes and across different sites, to raise the yield and reduce costs.

With more and more smart objects being connected, recent research on different trends of IoT shows direction toward many useful and highly beneficial topics including power and renewable energy systems. There is no doubt that renewable energy management at different scales can be made more effective in Egypt by the IoT paradigm. As Egypt is a country with an abundant supply of renewable energy, the ongoing improvements in power and renewable energy and increased efficiency can enable further benefits for Egypt from the IoT in the future. Energy production

and distribution can be easily monitored, and resultant advantages can be taken from improved speed and precision even at existing power levels.

Several opportunities exist to leverage the sensing and decision-making capabilities of the IoT to optimize the energy usage across a variety of consumers, raise the coordinated usage and planning of alternative energy sources, and reduce the overall energy and the currently large gap between the peak and the average consumption. Meanwhile, the building blocks of the IoT infrastructure for automated and machine-to-machine communication continue to be conventional. This revolution is characterized by connectivity solutions and end-to-end processing for industrial IoT.

The main idea of applying IoT in the industry is to move out of traditional ways of monitoring factories and collecting data into more automation and thus removing the physical distance limitations that currently exist. The concept here is that IoT-based technological innovations will enable to sense, process, and communicate with physical parameters in real time. Many applications and devices also exist that are suitable for industrial purposes. The overall view is to connect everything including humans to create pervasive cyber-physical digital environments.

This situation may well present an important opportunity for governments and organizations to play a greater role in providing solutions for Industrial IoT.

## References

1. Minerva R, Biru A, Rotondi D (2015) Towards a definition of the internet of things (IoT). *IEEE Internet Initiat* 1:1–86
2. Kiel D, Arnold C, Collisi M, Voigt K (2016) The impact of the industrial internet of things on established business models. In: *Proceedings of the 25th international association for management of technology (IAMOT) conference*
3. Striccoli D, Boggia G, Piro G, Grieco LA (2017) Cooperative networking techniques in the IoT age. In: *Internet of things*. Chapman and Hall/CRC, pp 51–69
4. Palattella MR, Dohler M, Grieco A, Rizzo G, Torsner J, Engel T, Ladid L (2016) Internet of things in the 5G era: enablers, architecture, and business models. *IEEE J Sel Areas Commun* 34(3):510–527
5. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Commun Surv Tutor* 17(4):2347–2376
6. Inácio PR, Freire MM, Correia AF, Sequeiros JB, Samaila MG (2017) IoT hardware development platforms: past, present, and future. In: *Internet of things*. Chapman and Hall/CRC, pp 107–139
7. Alioto M (2017) IoT: bird's eye view, megatrends and perspectives. In: *Enabling the internet of things*. Springer, pp 1–45
8. Mahalle PN, Raikar PN (2015) *Identity management for internet of things*, vol 39. River Publishers
9. Aitken R, Chandra V, Myers J, Sandhu B, Shifren L, Yeric G (2014) Device and technology implications of the internet of things. In: *2014 Symposium on VLSI technology (VLSI-technology): digest of technical papers*. IEEE, pp 1–4
10. Weber RH, Weber R (2010) *Internet of things*, vol 12. Springer
11. Bradley J, Barbier J, Handler D (2013) *Embracing the internet of everything to capture your share of \$14.4 trillion*. White Paper, Cisco

12. Majeed AA, Rupasinghe TD (2017) Internet of things (IoT) embedded future supply chains for industry 4.0: an assessment from an ERP-based fashion apparel and footwear industry. *Int J Supply Chain Manag* 6(1):25–40
13. Huang I, Guo R, Xie H, Wu Z (2012) The convergence of information and communication technologies gains momentum. *The global information technology report*, pp 35–45
14. Vermesan O, Friess P, Guillemin P, Serrano M, Bouraoui M, Freire L, Kallstenius T, Lam K, Eisenhauer M, Moessner K (2016) IoT digital value chain connecting research, innovation and deployment. *IERC Cluster, SRA*, pp 15–128
15. Di Martino B, Esposito A, Nacchia S, Maisto SA (2018) Towards an integrated internet of things: current approaches and challenges. In: *Internet of everything*. Springer, pp 13–33
16. Aloï G, Caliciuri G, Fortino G, Gravina R, Pace P, Russo W, Savaglio C (2017) Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. *J Netw Comput Appl* 81:74–84
17. Mikusz M (2014) Towards an understanding of cyber-physical systems as industrial software-product-service systems. *Proc CIRP* 16:385–389
18. Mourtzis D, Vlachou E, Milas N (2016) Industrial big data as a result of IoT adoption in manufacturing. *Proc CIRP* 55:290–295
19. Bilbao-Osorio B, Dutta S, Lanvin B (2013) *The global information technology report 2013*. In: *World Economic Forum*. Citeseer, pp 1–383
20. Chen CP, Zhang C-Y (2014) Data-intensive applications, challenges, techniques and technologies: a survey on big data. *Inf Sci* 275:314–347
21. Yi S, Hao Z, Qin Z, Li Q (2015) Fog computing: platform and applications. In: *2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb)*. IEEE, pp 73–78
22. Peralta G, Iglesias-Urkia M, Barcelo M, Gomez R, Moran A, Bilbao J (2017) Fog computing based efficient IoT scheme for the Industry 4.0. In: *2017 IEEE international workshop of electronics, control, measurement, signals and their application to mechatronics (ECMSM)*. IEEE, pp 1–6
23. Bonomi F, Milito R, Natarajan P, Zhu J (2014) Fog computing: a platform for internet of things and analytics. In: *Big data and internet of things: a roadmap for smart environments*. Springer, pp 169–186
24. Cristea V, Dobre C, Pop F (2013) Context-aware environments for the internet of things. In: *Internet of things and inter-cooperative computational technologies for collective intelligence*. Springer, pp 25–49
25. INFOSO D (2008) *Networked enterprise & RFID* INFOSO G. 2 micro & nanosystems, in cooperation with the Working Group RFID of the ETP EPOSS, internet of things in 2020, roadmap for the future [R]. Information Society and Media, Tech Rep
26. He J, Zhang Y, Huang G, Cao J (2012) A smart web service based on the context of things. *ACM Trans Internet Technol (TOIT)* 11(3):13
27. Castellani AP, Gheda M, Bui N, Rossi M, Zorzi M (2011) Web services for the internet of things through CoAP and EXI. In: *2011 IEEE international conference on communications workshops (ICC)*. IEEE, pp 1–6
28. Guinard D, Trifa V, Karnouskos S, Spiess P, Savio D (2010) Interacting with the SOA-based internet of things: discovery, query, selection, and on-demand provisioning of web services. *IEEE Trans Serv Comput* 3:223–235
29. Adly AS (2019) Climate change and energy decision aid systems for the case of Egypt. In: *Climate change and energy dynamics in the Middle East: modeling and simulation-based solutions. Understanding complex systems*. Springer International Publishing, Cham, pp 79–107. [https://doi.org/10.1007/978-3-030-11202-8\\_4](https://doi.org/10.1007/978-3-030-11202-8_4)
30. IEA I (2017) *International Energy Agency. Key world energy statistics*
31. Kabalci E, Gorgun A, Kabalci Y (2013) Design and implementation of a renewable energy monitoring system. In: *2013 fourth international conference on power engineering, energy and electrical drives (POWERENG)*. IEEE, pp 1071–1075

32. Goto Y, Ishiguro T, Kiya M, Mizutani Y, Sakai T, Kawagoe Y (2007) Integrated management and remote monitoring system for telecommunications power plants with fully DC-powered center equipment. In: 29th international telecommunications energy conference. INTELEC 2007. IEEE, pp 775–780
33. Suzdalenko A, Galkin I (2013) Case study on using non-intrusive load monitoring system with renewable energy sources in intelligent grid applications. In: 2013 8th international conference on compatibility and power electronics (CPE). IEEE, pp 115–119
34. Jiju K, Ramesh P, Brijesh P, Sreekumari B (2014) Development of android based on-line monitoring and control system for renewable energy sources. In: 2014 international conference on computer, communications, and control technology (I4CT). IEEE, pp 372–375
35. Kumar NM, Atluri K, Palaparthi S (2018) Internet of things (IoT) in photovoltaic systems. In: 2018 national power engineering conference (NPEC). IEEE, pp 1–4
36. Nkoloma M, Zennaro M, Bagula A (2011) SM 2: solar monitoring system in Malawi. In: Kaleidoscope 2011: the fully networked human? Innovations for future networks and services (K-2011), Proceedings of ITU. IEEE, pp 1–6
37. Duque E, González J, Restrepo J (2016) Developing sustainable infrastructure for small hydro power plants through clean development mechanisms in Colombia. *Proc Eng* 145:224–233
38. Fortaleza BN, Juan ROS, Tolentino LKS (2018) IoT-based pico-hydro power generation system using Pelton turbine. *J Telecommun Electr Comput Eng (JTEC)* 10(1–4):189–192
39. Chaturvedi P, Borah A, Singh A, Singh R (2018) IOT-Based Hydroenergy Generation with the Application of Sensors. In: *Intelligent Communication, Control and Devices*. Springer, pp 1225–1231
40. Amirat Y, Benbouzid MEH, Al-Ahmar E, Bensaker B, Turri S (2009) A brief status on condition monitoring and fault diagnosis in wind energy conversion systems. *Renew Sustain Energy Rev* 13(9):2629–2636
41. Lee KO, Chiang KS, Chen Z (2001) Temperature-insensitive fiber-Bragg-grating-based vibration sensor. *Opt Eng* 40(11):2582–2586
42. Kunzemann P, Jacobs G, Schelenz R (2017) Application of CPS within wind energy—current implementation and future potential. In: *Industrial internet of things*. Springer, pp 647–670
43. Kusiak A, Li W (2011) The prediction and diagnosis of wind turbine faults. *Renew Energy* 36(1):16–23
44. Wang L, Liu K-H (2007) Implementation of a web-based real-time monitoring and control system for a hybrid wind-PV-battery renewable energy system. In: *International conference on intelligent systems applications to power systems, 2007. ISAP 2007*. IEEE, pp 1–6

# Index

## 0-9

2.4GHz, 201, 216  
3D printing, 286  
3 stage IoT architecture, 167  
4G, 194  
5G, 194  
5G technology, 42  
6LoWPAN, 11

## A

Accreditation body, 83, 88, 95, 97, 99  
Accuracy, 125, 126  
Actuators, 227  
Adaptability, 231  
Advanced Message Queuing Protocol (AMQP), 18, 20, 23, 27, 28  
Advancements, 234  
Ambient, 264, 266, 268–270, 275, 277  
Ambient light sensing, 271  
Analog-digital converters, 127  
ANSI, 51  
Application layer, 306  
Architectural framework, 168  
Architecture, 56, 57, 61, 62, 64–67, 69–71, 75, 105, 262, 264, 265, 268, 270, 274, 277  
Architecture model, 107  
Architecture modeling, 112  
Artificial Intelligence (AI), 42, 263, 281, 285, 296  
Asset Efficiency (AE), 56, 62, 69, 72  
Asset management, 292  
Asset tracking, 292  
As smart energy, 249  
Asymmetric cryptography, 150  
Augmented personalised health, 263

Augmented reality, 164, 165, 183, 185, 187, 188  
Automated calibration, 90–92, 97  
Automated transportation, 233  
Automated warehouses, 293  
Automation, 35–38, 40, 303  
Automation level, 123–125, 127, 129, 131, 133, 134, 136, 137  
Automation pyramid, 121–124, 126, 131–137  
Autonomous ground carts, 180  
Autonomous vehicles, 158  
Aviation, 36, 39

## B

Battery storage, 239  
Battery technology, 224, 235  
Bi-channel communication, 229  
Big data, 42, 147, 281, 310  
Bigdata analytics, 145  
Bitcoin, 149  
Bitcoin blockchain, 149  
Block, 149  
Blockchain, 145, 146, 149, 151–154, 156–160, 285  
Blockchain platform, 153, 155–157  
Blue chip radiation, 171  
Body sensors, 268  
Building Automation System (BAS), 237  
Building Internet of Things (BIoT), 244  
Buildings, 237  
Business plan, 238  
Business process management, 137  
Business Process Management Maturity (BPMM), 137  
Buyers, 249

**C**

Cameras, 172  
 Carbon emission, 227, 248, 256  
 Carbon emission reduction, 248  
 Case studies, 227  
 Challenge, 299, 304, 311  
 Channel state information, 306  
 Cisco, 228, 280  
 Cloud, 29, 196, 202, 207, 208  
 Cloud based service, 227  
 Cloud computing, 56, 57, 64, 65, 276, 277  
 Cloud service, 91, 94–97  
 Cloud storage, 145  
*Commercial Off-The-Shelf (COTS)*, 136  
 Communication, 300–303, 305, 308–310, 312–314  
 Communication model, 107  
 Competitiveness, 121–123, 125, 126, 128–131, 133, 135–137  
 Condition monitoring, 287, 288  
 Condition Monitoring System (CMS), 315  
 Confidentiality, 129, 130  
 Connected devices, 232  
 Connected tools, 286, 293  
 Connected workforce, 295  
 Connectivity, 129, 131, 136, 148, 230–232  
 Connectivity issues, 284  
 Connectivity performance, 128, 130  
 Constrained Application Protocol, 23  
 Context awareness, 268  
*Control level*, 123, 126, 128  
 Conventional grid, 230, 241, 253  
 Conventionally, utilities, 236  
 Conventional wiring, 231  
 CORBA, 107  
 Cost-Effectiveness, 121, 133, 135–137  
 Cryptocurrency, 150  
 Cryptographic hash functions, 150  
 Customer Relationship Management (CRM), 305  
 Cyber-attacks, 145, 147, 148  
 Cyber Physical Systems (CPS), 60, 64, 67, 268, 281, 308, 314  
 Cyber security, 150, 156, 283, 285  
 Cycle time monitoring, 288

**D**

Data, 304, 305, 314, 316  
 Data accuracy, 132  
 Datacenter, 107, 108, 110  
 Data Centric Publish/Subscribe (DCPS), 108  
 Data Distribution Service (DDS), 103–105, 107–118

Data distribution service for real-time systems, 104  
 Data distribution specification, 110, 111  
 Data exchange, 104  
 Data leaching, 285  
 Data Local Reconstruction Layer (DLRL), 109, 110  
 Data standardization, 92  
*Data Writers*, 108  
 DDS UML Profile, 105, 110–114, 116, 117  
 Decentralized, 149  
 Demand charges, 237  
 Demand management, 225, 246  
 Denial of Service (DoS), 305  
 Development, 4, 8, 10, 25, 27  
 Device control, integration and simulation, 24  
 Device EUI, 208  
 Device to Device (D2D), 228  
 Device under test, 85, 86  
 Digital thread, 69, 72  
 Digital twins, 25  
 Directory services, 104  
 Discrete process, 126, 128  
 Distributed, 149  
 Distributed control, 126  
 Distributed Control Systems (DCS), 169  
 Distributed energy, 241, 245  
 Distributed Energy Resources (DER), 241  
 Distributed generation, 242  
 Distributed Interactive Simulation (DIS), 105  
 Distributed system, 104  
 Distribution service, 103–105, 107, 110, 117  
 Domain, 107  
 Domain Participant, 108  
 Drones, 169

**E**

ECDSA, 151  
 Eclipse, 7, 24–27  
 Eclipse graphical modeling framework, 110  
 Efficacy, 257  
 Efficiency, 35, 37, 38, 41, 47, 51  
 Efficiency management, 122  
 Egypt, 299–304, 308, 309, 311–313, 315, 316  
 Electrical grid, 236  
 Electricity, 223, 225, 226, 230, 234–244, 246–249, 254–257  
 Electric vehicles, 230, 241–243, 249  
 Electrodermal activity, 266  
 Electromyography, 266  
 Electronic test equipment, 82, 85, 86, 88  
 End-to-end IoT solution, 4, 7, 29  
 Energy, 194, 198, 199, 300, 313–316



Energy efficacy, 243, 249  
 Energy efficiency, 125, 126  
 Energy harvesting receivers, 173  
 Energy industry, 223, 226, 251, 256  
 Energy production, 224, 226, 234, 240, 248–250, 252  
 Energy trading platform, 229  
 Energy utilization, 223, 226, 251, 256  
*Enterprise level*, 124  
 Enterprise Resource Planning (ERP), 55, 59–62, 64, 69–72, 131, 304  
 Enterprises, 193, 194, 214, 216  
 Environmental monitoring, 233  
 Ethereum Virtual Machine (EVM), 156  
 EV batteries, 254  
 eXtensible Messaging and Presence Protocol (XMPP), 18, 20, 23

## F

Fault tolerance, 230  
 Feature diagram, 105  
*Field level*, 123, 124, 126  
 Fog computing, 310  
 Fossil fuel, 223, 224, 235, 236, 251, 256  
 Four-Step-Rule-Set (4SRS), 66  
 Fourth Industrial Revolution, 262, 284, 296, 308  
 Frequency bands, 195, 197  
 Fuel cells, 242  
 Future, 305, 311, 313, 314

## G

Gateway, 196, 198, 199, 201, 203–205, 208  
 GDP, 233  
 Geothermal, 224, 235, 236, 249  
 GIS-based visualization, 257  
 Google, 51  
 GPIB/IEEE-488, 87  
 GPS, 292  
 Graphic prototypes, 286  
 Grid infrastructure, 237  
 Grid Interactive Electric Thermal Storage (GETS), 252  
 GSM, 229, 266, 313  
 GSM, 232, 233

## H

Hashing, 150, 152  
 Healthcare, 38, 39, 41, 261–277  
 High Level Architecture (HLA), 105, 107  
 HVAC, 244  
 Hybrid microgrid, 229  
 Hydro energy, 313  
 Hydropower, 224, 235

## I

IBM Watson, 29  
 ICG, 268  
 IEEE, 51, 194, 200  
 IEEE-802, 11  
 I4.0, 55, 58, 62, 63, 65, 70, 73, 300, 308  
 IMP\_4.0, 57–60, 63, 66, 67  
 Industrial, 199, 200  
 Industrial automation, 124  
 Industrial Digital Twin (IDT), 56, 62, 69, 70, 72  
 Industrial internet, 4–7, 35–39, 42, 51, 165  
 Industrial Internet Connectivity Framework (IICF), 6  
 Industrial Internet Consortium (IIC), 6, 280  
 Industrial Internet of Things (IIoT), 5, 6, 35–44, 48, 49, 51, 55–58, 62, 63, 65, 70–73, 104, 145–149, 151–160, 165, 225–228, 231, 235, 245, 248, 251, 253, 255, 256, 279–286, 288, 292–296  
 Industrial Internet of Underwater Things (IIoUT), 186  
 Industrial Internet Reference Architecture (IIRA), 6, 56–59, 65, 67, 70, 168  
 Industrial processes, 127, 129, 134–137  
 Industrial revolution, 146, 147  
 Industrial robotics, 169  
 Industrial Wireless Networks (IWNs), 37  
 Industrie 4.0, 5, 7  
 Industry, 299, 316  
 Industry 4.0, 4, 5, 36–39, 48, 51, 146, 147, 165, 187, 280, 281, 285, 296, 300, 308  
 Information, 304, 307–309, 314  
 Intelligent digital meters, 226  
 Intelligent Electronic Devices (IED), 26  
 Intelligent switches, 226, 248, 250  
 Intelligent transport, 163  
 Interconnectivity, 282  
 International Society of Automation (ISA), 40  
 Internet, 299, 300  
 Internet of industrial things, 4  
 Internet of Things (IoT), 5, 7, 35–42, 44, 46, 47, 51, 55, 60, 61, 64, 65, 69, 104, 147, 165, 193–195, 197–204, 206, 207, 216, 224–233, 240, 241, 244–246, 248, 252, 253, 255–257, 299–317  
 Internet of Things Consortium (IoTC), 7  
 Interoperability, 4, 55, 57, 58, 60, 70, 72–75, 307  
 In-vehicle Google mapping, 41  
 IoT gateways, 286, 289, 291, 292  
 IoT sensors, 164  
 IPv6, 38  
 ISA-95, 58, 60, 70, 72

ISO, 51

ITU, 51

## J

Java Message Service (JMS), 105, 107

## K

KHealth, 263

## L

Laser diodes, 164, 173

Law enforcement, 165, 188

LED-based IIoT sensor data transmissions, 183

LED beaconing, 163, 164, 188

Light Emitting Diodes (LED), 163–165,  
170–179, 181–188

Light Fidelity (Li-Fi), 170, 181, 186

Line of sight, 173–175, 180, 182

Load management algorithm, 229

Logical topology, 122, 133, 134, 136

Logic controller, 123

Logistics, 47, 156, 292

LoRa, 11, 195, 197–204, 214, 216

LoRaWAN, 195–198, 201–203, 206, 208

Low Power Wide Area (LPWA), 194, 216

Low Power Wide Area Network (LPWAN),  
195, 216

LTE-M communication, 46

## M

Machine learning, 181

Machine-to-Machine (M2M), 11, 18, 23, 28,  
29, 36, 37, 166, 180, 183, 301

Maintenance, 160

Manufacturing, 36, 40, 81, 82, 84, 122, 124,  
125, 130–132, 136, 145, 147, 148, 156,  
158, 160

Manufacturing Execution Systems (MES), 55,  
59, 62, 64, 69, 72, 128

Manufacturing industry, 233

Manufacturing intelligence, 304

Matlab, 270

Measurement uncertainty, 84, 86, 95, 96

Mechanocardiography (MCG), 268

Message Queuing Telemetry Transport  
(MQTT), 18, 19, 22–25, 28, 29, 228

Metamodel, 110, 111

MHealth, 263

Micro-electro-mechanical systems, 178

Micro-LEDs, 171

Microservices, 66, 67, 71, 72

Micro-turbines, 242, 249

Middleware, 103–105, 107, 115, 117, 264–266

MIMO, 176, 179, 181

MISO, 176

Mobile health, 169

Modality, 267, 268

Monitoring system, 44

Multiagent system, 229

## N

Nano-grids, 242

Network, 193–198, 201, 202, 210, 216, 300,  
301, 306, 309

NIST SM, 56, 58, 59, 73

Non-accessibility, 255

Normative standard, 91, 92

Nuclear, 236

## O

OASIS, 18

Object Management Group (OMG), 7, 104,  
109–111, 117

Object model, 107

Object naming service, 307

Open Connectivity Foundation (OCF), 7

Open Platform Communications Unified  
Architecture (OPC UA), 22, 23, 27

OpenHAB, 24, 26

OpenWrt Router, 11

Operational efficiency, 223, 256

Operation management, 128

Opportunity, 254

Optical camera communications, 172

Optical spectrum, 175

Optimization, 246

Organic Light Emitting Diodes (OLED), 171

## P

Parking Detection Sensor, 109

Peak demand, 236, 237, 239, 240

Performance test, 85, 86

Pharmaceutical, 36, 39, 40, 47

Phosphor coated blue-chips, 171

Photodetectors, 171, 172

Photomultiplier tubes, 173

Photo resistor, 271

Photovoltaic, 313

PIR motion sensor, 271

Planning level, 124, 129, 130

Platforms, 23, 29

Plattform Industrie 4.0, 6

Plug-in hybrid vehicles, 249

Power, 302, 303, 305, 310, 313–315

Power Tower, 252

Power wastage, 230

Predictive maintenance, 40, 41, 47, 147, 159,  
225, 227, 256, 288

- Preventive maintenance, 279, 288, 290
- Privacy and confidentiality, 276
- Process Control and Safety Forum, 40
- Product Lifecycle, 305
- PRODUTECH-SIF, 57, 62, 64, 67–69, 72–74, 76
- Protocol, 9, 18, 19, 195, 200, 202, 204
- Prototypes, 257
- Public Key Asymmetric algorithms, 285
- Public key cryptography, 150
- Publisher*, 108
- Publish-subscribe architecture, 105
- Publish/subscribe middleware, 104
- Publish/subscribe pattern, 104, 105
  
- Q**
- QLEDs, 171
- QoS Policies, 111
- Quality management, 291, 292
- Quality of Service (QoS), 108–111, 116, 117
- Quality standards, 291
- Quick fluctuations, 251
  
- R**
- Radio frequency, 163, 188
- Radio-Frequency Identification (RFID), 43, 45, 51, 156, 286, 292, 293, 301
- RAMI 4.0, 6, 57, 59, 67, 168
- Random Phase Multiple Access (RPMA), 216
- Raspberry, 203
- Raspberry pi 3, 230
- Rational Unified Process, 112
- Real-time pricing, 230
- Reference architecture, 4, 7
- Reference Architecture Model Industrie 4.0, 6, 168
- Reference architectures, 5, 168
- Reliability, 37, 38, 89, 97, 100, 147, 148, 150, 158, 160, 239, 246, 248, 255, 306
- Remote monitoring, 225, 230, 256
- Remote Terminal Unit (RTU), 123
- Renewable electrical energy, 240
- Renewable energy, 223–226, 229, 230, 234, 235, 238–240, 246, 248, 249, 251–253, 255–257, 312–314, 316
- Requirements, 55–57, 63–66, 70, 71, 75
- Resilience level, 128, 130
- Response time, 125, 126, 131, 132
- RESTful APIs, 309
- RF communications, 175, 176
- RF transmitters, 282
- Robotic, 38, 39, 51, 286
- Robots, 286, 292–294
  
- S**
- SaaS, 43
- Safety, 233
- Scalability, 104, 115, 127, 128
- Scope of accreditation, 83, 88, 92, 96, 97
- SCPI/IEEE488.2, 87
- Security, 127, 128, 132, 305, 311
- Self-healing, 230
- Semantic interoperability, 57, 62, 63, 72–76
- Sensor, 3, 9, 109, 200, 227, 228, 230, 233, 235, 244, 246, 248, 250, 252, 301, 302, 309, 313–315
- Sensors and actuators, 153
- Sensor technology, 256
- Sigfox, 11
- Signal to noise ratio, 306
- Single-Board Computer (SBC), 153
- Single point of failure, 307
- Situational awareness, 229
- Smart city, 109, 199, 200
- Smart city engineering, 109
- Smart city governance, 262
- Smart contracts, 151, 152
- Smart decisions, 122–124, 126, 130–132
- Smart equipment, 246
- Smart factories, 36, 39, 48, 51, 279–281, 285, 286, 293
- Smart farming, 164, 165, 188
- Smart gadgets, 227
- Smart grid, 223–226, 230, 233, 241, 245–247, 253–256
- Smart home, 25, 232
- Smart home agents, 229
- Smart meters, 169, 229, 249, 250
- Smart microgrid, 223–226, 234, 248–250, 254–256
- Smart sensors, 38
- Smart Traffic System (STS), 103, 109
- SoaML, 66, 68
- Solar arrays, 242
- Solar cells, 173, 175
- Solar photovoltaic, 230, 239
- Solar PV, 239–243, 245
- Speed, 244
- Speed Camera, 109
- Standardization, 284

Standards, 4, 8, 11, 12, 18, 19  
 STEP, 72  
 STEP-NC, 74  
 Subscriber, 108  
 Supervisory Control and Data Acquisition (SCADA), 22, 23, 28, 128–130, 169, 315, 316  
 Supervisory level, 123, 127, 128, 130  
 Supply chain, 36, 41, 122, 137, 157, 165  
 Supply Chain Management (SCM), 157  
 System, 307, 311–313, 315

**T**

Technical interoperability, 57, 63, 70–72, 76  
 Technology, 249, 300, 308, 316  
 Temboo, 28  
 Testing certificate, 92  
 Testing terminal, 86, 90  
 Test point, 85, 91, 96–98  
 Test setup, 85–87, 96  
 Thing, 3, 8, 9, 300, 301, 308, 311, 312  
 Things Network (TTN), The , 198, 203, 204, 206–208  
 ThingSpeak, 266, 270, 271  
 Three-tier, 65, 67–69  
 Topic, 108  
 Traceability chain, 84, 92  
 Transactions, 145, 149–152, 154–157, 160  
 Transaction services, 104  
 Transparency, 149, 156  
 Transportation, 38–41, 43  
 Transportation industry, 164, 165, 188  
 Trust, 303

**U**

Ubiquitous computing, 163, 165, 184, 188, 228  
 UH4SP, 57, 58, 60, 61, 64, 66, 68, 72  
 Uncertainty calculation, 97, 99  
 Universal Modelling Language (UML), 64, 66, 103–105, 110–117

University, 193, 201  
 Unobtrusive, 261, 262, 266, 277  
 USB, 9  
 Urban security, 233

**V**

Value chain, 36, 39  
 Vehicular ad hoc Networks (VANET), 302  
 Virtual reality, 38  
 Visible Light Communication (VLC), 163–165, 170–188  
 Visible light sensing, 177, 188  
 VLC for smart farming, 185  
 VLC receivers, 171  
 VLC transmitters, 170–172, 175, 185, 186, 188

**W**

Wearable, 261, 264, 266–268, 270, 271, 273, 275  
 Wide Area Network (WAN), 166, 168  
 Wi-Fi, 194, 199, 201  
 WiMAX, 11, 15  
 Wind energy, 314  
 Wireless, 194, 195, 197–201, 204, 214, 216  
 Wireless Body Area Networks (WBAN), 184  
 Wireless communications, 170, 174, 179, 182, 183  
 Wireless medical sensor networks, 42  
 Wireless Sensor Networks (WSN), 257  
 Worker safety, 295

**X**

XBee, 270

**Z**

Zero energy buildings, 238  
 Zero energy receivers, 174  
 ZigBee, 11, 13, 18, 28, 265