Premier Reference Source

5G Internet of Things and Changing Standards for Computing and Electronic Systems

Augustine O. Nwajana

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

5G Internet of Things and Changing Standards for Computing and Electronic Systems

Augustine O. Nwajana
University of Greenwich, UK

A volume in the Advances
in Computer and Electrical
Engineering (ACEE) Book Series

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

Published in the United States of America by
IGI Global
Engineering Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Nwajana, Augustine Onyenwe, 1979- editor.
Title: 5G internet of things and changing standards for computing and electronic systems / Augustine O. Nwajana, editor.
Description: Hershey, PA : Engineering Science Reference, [2022] | Includes bibliographical references and index. | Summary: "The emphasis of this book is on the seamless connectivity due to the development of the IoT technology and how each technology works and impacts the development of the emerging global smart city"-- Provided by publisher.
Identifiers: LCCN 2022970002 (print) | LCCN 2022970003 (ebook) | ISBN 9781668438558 (h/c) | ISBN 9781668438565 (s/c) | ISBN 9781668438572 (ebook)
Subjects: LCSH: Internet of things. | 5G mobile communication systems.
Classification: LCC TK5105.8857 .A167 2022 (print) | LCC TK5105.8857 (ebook) | DDC 004.67/8--dc23/eng/20220301
LC record available at https://lccn.loc.gov/2022970002
LC ebook record available at https://lccn.loc.gov/2022970003

This book is published in the IGI Global book series Advances in Computer and Electrical Engineering (ACEE) (ISSN: 2327-039X; eISSN: 2327-0403)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material.
The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Advances in Computer and Electrical Engineering (ACEE) Book Series

ISSN:2327-039X
EISSN:2327-0403

Editor-in-Chief: Srikanta Patnaik, SOA University, India

MISSION

The fields of computer engineering and electrical engineering encompass a broad range of interdisciplinary topics allowing for expansive research developments across multiple fields. Research in these areas continues to develop and become increasingly important as computer and electrical systems have become an integral part of everyday life.

The **Advances in Computer and Electrical Engineering (ACEE) Book Series** aims to publish research on diverse topics pertaining to computer engineering and electrical engineering. **ACEE** encourages scholarly discourse on the latest applications, tools, and methodologies being implemented in the field for the design and development of computer and electrical systems.

COVERAGE

- Analog Electronics
- Circuit Analysis
- Computer Architecture
- Microprocessor Design
- Chip Design
- Power Electronics
- Digital Electronics
- Algorithms
- Electrical Power Conversion
- Computer Science

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: http://www.igi-global.com/publish/.

The Advances in Computer and Electrical Engineering (ACEE) Book Series (ISSN 2327-039X) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/advances-computer-electrical-engineering/73675. Postmaster: Send all address changes to above address.

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

701 East Chocolate Avenue, Hershey, PA 17033, USA
Tel: 717-533-8845 x100 • Fax: 717-533-8661
E-Mail: cust@igi-global.com • www.igi-global.com

To My Lovely Daughter – Munachimso Jess Onyenwe.

Table of Contents

Section 2
Electronic Science and Engineering

Detailed Table of Contents

Section 1
Computing and Software Engineering

The Internet of Things (IoT) is an emerging computing paradigm that supports the interconnection of objects. With the rapid growth in smart technologies, IoT is gaining popularity from industry and academia focusing on communication and networking of smart objects. It is assumed that in a typical IoT application, the smart sensors are capable of directly delivering a service with no or minimal human involvement. There are many new technologies that are driving the development of IoT, which include cloud computing, wireless sensor networks, and 5G, etc. On the other hand, there are many research challenges that need to be addressed such as identity management of billions of devices connected to the internet, standardization, privacy, energy management, security of the information, space to store and process the information, etc. In this regard, the main focus of this chapter is to present IoT in a broader perspective and its associated technologies and applications along with a review of the work published in these areas.

The AssessLIFE software is a solution platform that analyzes and reveals if industrial physical assets made of metals, alloys, and welds can survive their exposure or ambient conditions. The software also reveals when time-dependent premature failure is likely to occur. The software can generate great financial and safety benefits for all stakeholders. Furthermore, the AssessLIFE software aims to provide asset information for better financial and technical decision-making by managers, engineers, legal teams, insurance teams, fabricators, and inspectors.

Healthcare is an important part of every individual's life. Unfortunately, the rising prevalence of chronic diseases is putting a burden on the modern healthcare system. The internet of things (IoT) with 5G technology offers a number of advantages to the healthcare system, including remote monitoring, remote robotic surgery, and ambulances operating on dedicated network slices, all of which relieve pressure on the traditional healthcare system. 5G-IoT enables billions of healthcare equipment to communicate with one another. These devices will produce a huge amount of data that can be evaluated. In the healthcare industry, data analytics has a huge potential. In this chapter, the authors examine a brief history of machine learning as well as some fundamental knowledge of the methodologies. In addition, the author has provided a brief overview of several machine learning algorithms utilized in healthcare in the context of 5G-IoT. The future aspect of machine learning in a 5G-IoT smart healthcare system was also highlighted.

Risk management plays a vital role in tackling cyber threats within the cyber-physical system (CPS) for overall system resilience. It enables identifying critical assets, vulnerabilities, and threats and determining suitable proactive control measures to tackle the risks. However, due to the increased complexity of the CPS, cyber-attacks nowadays are more sophisticated and less predictable, which makes risk management task more challenging. This chapter proposes an integrated cyber security risk management (i-CSRM) framework for systematically identifying critical assets through the use of a decision support mechanism built on fuzzy set theory, predicting risk types through machine learning techniques, and assessing the effectiveness of existing controls through the use of comprehensive assessment model (CAM) parameters.

Orthogonal frequency division multiplexing (OFDM) is a multi-carrier transmission technique used to accomplish high data rate transmission in wireless communications. OFDM is one of the major players of multi-carrier communication systems in 5G networks due to its high spectral efficiency and is immune to multipath fading. However, the OFDM signal suffers from significant amplitude fluctuations resulting in a large peak-to-average power ratio (PAPR), which is one of the main downsides of OFDM systems. Therefore, limiting the PAPR in OFDM systems is a key issue, as decreasing PAPR results in lower power consumption and hence an extended battery life. Reducing PAPR without degrading power usage efficiency and bit error rate (BER) is a challenging issue in improving communication performance. This chapter discusses the use of compressive sensing for PAPR reduction in OFDM systems to deploy in energy-efficient 5G networks.

In this study, firstly, a dataset of 10,476 annotated vulnerable ERC-20 standard token smart contracts (belonging to a set of 33 common smart contract vulnerabilities) has been collected from a publicly available repository. Secondly, using the SolMet smart contract metrics measurement tool, the object-oriented software attributes (i.e., metrics) from each smart contract's source code has been extracted. Lastly, using the source code metrics and the vulnerability annotations (i.e., labels) as the input in supervised machine learning (classification) algorithms, the accuracy of each individual algorithm is evaluated against the accuracy of an ensemble classifier (namely voting). The model accuracies demonstrate the feasibility of identifying and prioritising smart contracts for further inspection prior to deployment to the blockchain network. The ensemble classifier performed better (accuracy = 0.79) compared to each classifier when used individually.

Preface

Internet of things networks have changed the standard of how computing and electronic systems are interconnected. Computing and electronic devices and systems, with the help of 5G technology, can now be seamlessly linked in a way that is rapidly turning the globe into a digital world. Smart cities and the internet of things are here to stay but not without some challenges; a thorough review of the opportunities, difficulties, and benefits of 5G internet of things is necessary for it to be successfully utilized and implemented.

The *5G Internet of Things and Changing Standards for Computing and Electronic Systems* examines modern computers and electronics and how they provide seamless connectivity due to the development of internet of things technology. Moreover, this reference covers various technologies and their roles and impacts in the future of smart cities. Covering a range of topics such as machine learning and renewable energy systems, this reference work is ideal for scientists, engineers, policymakers, researchers, practitioners, academicians, scholars, instructors, and students.

The book is organized in two sections and 10 chapters. The first section (Section 1) contains seven chapters covering selected topics in computing and software engineering. The second section (Section 2) holds three chapters covering selected topics in electronic science and engineering. A brief description of each chapter is given below:

Chapter 1 covers recent advancements on the Internet of Things (IoT). The IoT is an emerging computing paradigm that supports the interconnection of objects. With the rapid growth in smart technologies, IoT is gaining popularity from Industry and academia focusing on communication and networking of smart objects. It is assumed that in a typical IoT application the smart sensors are capable of directly delivering a service with no or minimal human involvement. There are many new technologies that are driving the development of IoT, which include, cloud computing, wireless sensor networks, etc. On the other hand, there are many research challenges that need to be addressed such as identity management of billions of devices connected to the internet, standardization, privacy, energy management, security of the information, space to store and process the information, etc. In this regard, the focus of this chapter is to present the IoT in a broader perspective and its associated technologies, and applications along with a review of the work published in these areas.

Chapter 2 focuses on the development of a new software termed AssessLIFE. The AssessLIFE software is a solution platform that analyzes and reveals if industrial physical assets made of metals, alloys, and welds can survive their exposure or ambient conditions. The software also reveals when time-dependent pre-mature failure is likely to occur. The software can generate great financial and safety benefits for all stakeholders. Furthermore, the AssessLIFE software aims to provide asset information for better financial and technical decision-making by managers, engineers, legal teams, insurance teams, fabricators, and inspectors. The beneficiaries of asset lifespans and analytics on degradation drivers generated by the AssessLIFE software include, but are not limited to managers, legal teams, insurance teams, engineers, fabricators, and inspectors. The main points which the AssessLIFE software addresses with solutions include but are not limited to asset safety and health assessment, production loss, maintenance cost overruns, legal assessment, insurability assessments, engineering decision-making, and fabrication decision-making.

Chapter 3 discusses "A Network Data Analytic Technique in 5G-IoT-Based Smart Healthcare System Using Machine Learning." Healthcare is an important part of every individual's life. Unfortunately, the rising prevalence of chronic diseases is putting a burden on the modern healthcare system. The Internet of Things (IoT) with 5G technology offers several advantages to the healthcare system, including remote monitoring, remote robotic surgery, and ambulances operating on dedicated network slices, all of which relieve pressure on the traditional healthcare system. 5G-IoT enables billions of healthcare equipment to communicate with one another. These devices will produce a huge amount of data that can be evaluated. In the healthcare industry, data analytics has a huge potential. In this chapter, the authors examine a brief history of machine learning as well as some fundamental knowledge of the methodologies. In addition, the author has provided a brief overview of several machine learning algorithms utilized in healthcare in the context of 5G-IoT. The future aspect of machine learning in a 5G-IoT smart healthcare system was also highlighted.

Chapter 4 presents the "Protection of Critical Infrastructure Using an Integrated Cybersecurity Risk Management (i-CSRM) Framework." Risk management plays a vital role in tackling cyber threats within the Cyber-Physical System (CPS) for overall system resilience. It enables identifying critical assets, vulnerabilities, and threats and determining suitable proactive control measures to tackle the risks. However, due to the increased complexity of the CPS, cyber-attacks nowadays are more sophisticated and less predictable, which makes risk management task more challenging. This chapter proposes an Integrated Cyber Security Risk Management (i-CSRM) framework for systematically identifying critical assets using a decision support mechanism built on fuzzy set theory, predicting risk types through machine learning techniques, and assessing the effectiveness of existing controls through the use of comprehensive assessment model (CAM) parameters.

Chapter 5 investigates “PAPR Reduction in OFDM Systems Using Compressive Sensing for Energy Efficient 5G Networks Compressive Sensing.” Orthogonal frequency division multiplexing (OFDM) is a multi-carrier transmission technique used to accomplish high data rate transmission in wireless communications. OFDM is one of the major players of multi-carrier communication systems in 5G networks, due to its high spectral efficiency and is immune to multipath fading. However, the OFDM signal suffers from significant amplitude fluctuations resulting in a large peak-to-average power ratio (PAPR), which is one of the main downsides of OFDM systems. Therefore, limiting the PAPR in OFDM systems is a key issue, as decreasing PAPR results in lower power consumption and hence an extended battery life. Reducing PAPR without degrading power usage efficiency and bit error rate (BER) is a challenging issue in improving communication performance. This chapter discusses the use of compressive sensing for PAPR reduction in OFDM systems, to deploy in energy efficient 5G networks.

Chapter 6 proposes the “Prediction of Ethereum Blockchain ERC-20 Token Standard Smart Contract Vulnerabilities Using Source Code Metrics.” The study, a dataset of 10,476 annotated vulnerable ERC-20 standard token smart contracts (belonging to a set of 33 common smart contract vulnerabilities) is collected from a publicly available repository. Using the SolMet smart contract metrics measurement tool, the object-oriented software attributes (i.e., metrics) from each smart contract’s source code is extracted. Lastly, using the source code metrics and the vulnerability annotations (i.e., labels) as the input in supervised machine learning (classification) algorithms, the accuracy of each individual algorithm is evaluated against the accuracy of an ensemble classifier (namely Voting). The model accuracies demonstrate the feasibility of identifying and prioritising smart contracts for further inspection prior to deployment to the blockchain network. The ensemble classifier performed better (accuracy = 0.79) compared to each classifier when used individually.

Chapter 7 presents an application-oriented survey on adaptability of artificial intelligence for natural language processing. The application domains for Artificial Intelligence and machine learning are expanding exponentially in recent times.

The domains such as automation in software and business processes, healthcare, agriculture, robotics, and mostly natural language processing have seen the most adaptations. The domain of natural language processing seeks the maximum adaptation due to various sub domain applications such as textual classification, detection of emotions, design and delivery of virtual assistant tools, extraction of knowledge, content summarization, content recommendations, user profiling for content consumption habits, grammar and dialect verification and text summation. These subdomains cater to a wide range of purposes such as user profiling or emotion extraction for surveying or feedback analysis for data driven applications.

Chapter 8 focuses on RF/microwave instruments evolution, from professional hardware into amateur kit and software-defined radio. The chapter describes the evolution of RF/microwave instruments within two decades. The described RF/microwave instruments focus more on low-cost amateur RF signal sources, power detectors, spectrum analyzers (SA), vector network analyzers (VNA), and software-defined radios (SDR). Each instrument is introduced, and its uses are compared. The chapter also reviews the development history and development factors of amateur RF/microwave instruments in the past twenty years. Through this chapter, fresh RF/microwave amateurs and hobbyists will better understand the development of low-cost instruments in the present and in the future, as well as provide guidelines for RF/microwave amateurs and hobbyists in the selection and purchase of such instruments. In fact, some amateur instruments are also used in 5G research and IoT applications when considering their instrument size, research budget, and the need to use many instruments in the application.

Chapter 9 investigates tuneable attenuator based on hybrid metal-graphene structure on spoof surface plasmon polaritons waveguide. A new type of tuneable attenuator on spoof surface plasmon polaritons (SSPP) waveguide based on hybrid metal-graphene structure for terahertz applications is proposed in this paper. Two structures are analyzed and designed, where the first is composed of a graphene sheet at only one cell of the SSPP waveguide and the second at all cells. By varying the graphene chemical potential via a biased voltage, the surface conductivity of Graphene can be adjusted. Therefore, the attenuation can also be adjusted. Moreover, an equivalent circuit model is proposed to facilitate the designs of the proposed attenuator and offer a general understanding of the attenuation mechanism. Numerical simulation results with the CST simulator and WCIP method have a good agreement with the theoretical results. The simulated results show that the attenuator can obtain an adjustment range from 6.02 to 14.32 dB for the first structure and from 1.58 to 30.93 dB for the second, as the chemical potential rises from 0 to 0.5 eV.

Chapter 10 discusses the opportunities and challenges for VLSI in IoT applications. IoT systems combine sensing, computation, storage, and communication to sense physical systems and respond accordingly. However, larger size chips are not suitable for fog and edge devices. Therefore, a new mindset is required for VLSI design to implement the IoT application. This chapter describes the first conventional technology used in VLSI design. Afterward, the characteristics of IoT systems relevant to VLSI design identify essential factors and challenges at different levels. Finally, the fifth-generation network (5G) is also studied to expand IoT applications.

Augustine O. Nwajana
University of Greenwich, UK

Section 1

Computing and Software Engineering

Chapter 1

Internet of Things:
A Broader View of Architecture, Key Technologies, and Research Opportunities

Payaswini P.
https://orcid.org/0000-0002-4711-7690
Goa University, India

ABSTRACT

The Internet of Things (IoT) is an emerging computing paradigm that supports the interconnection of objects. With the rapid growth in smart technologies, IoT is gaining popularity from industry and academia focusing on communication and networking of smart objects. It is assumed that in a typical IoT application, the smart sensors are capable of directly delivering a service with no or minimal human involvement. There are many new technologies that are driving the development of IoT, which include cloud computing, wireless sensor networks, and 5G, etc. On the other hand, there are many research challenges that need to be addressed such as identity management of billions of devices connected to the internet, standardization, privacy, energy management, security of the information, space to store and process the information, etc. In this regard, the main focus of this chapter is to present IoT in a broader perspective and its associated technologies and applications along with a review of the work published in these areas.

DOI: 10.4018/978-1-6684-3855-8.ch001

INTRODUCTION

The present world is moving towards automation and digitization leading to the concept of digital life with less human involvement. A rapid growth in Internet and wireless network technologies has played a major role in this shift towards the digital era. Before the birth of the internet, the control of the process was mainly handled by humans and would take a longer time for the execution of jobs. Now, with the availability of advanced technologies, the main goal is to minimize human interaction and allow Machine to Machine interaction to control and effectively deliver the application service. This has led to the introduction of concepts such as Wireless Control, Remote Monitoring, etc. Furthermore, with the introduction of the concept of intelligent computing a new field called the Internet of Things (IoT) has evolved (Gubbi et al.,2013; Yi & Liang, 2010).

IoT is an emerging computing paradigm that enables the connecting of sensors, actuators, and other smart technologies for person-to-object and object-to-object communications (Yi & Liang, 2010). The basic idea of IoT is to allow smart sensors to communicate directly to deliver a service without human involvement. According to the authors in (Ma, 2011), IoT is defined as "a network that interconnects ordinary physical objects with the identifiable addresses that provide intelligent services". Due to the advancements in the technologies such as RFID, Wireless Sensor Networks (WSN), Near Field Communication (NFC), communication technologies, and Internet protocols, IoT has gained huge popularity in industry and academia (Gubbi et al.,2013). WSNs are playing a major role as it is cheaper and provides support to Internet-connected devices. Moreover, the wearable and implanted sensors are becoming part of our daily life and have contributed to the development of IoT applications in digital healthcare, home automation, etc.

According to Statista (Arne Holst, 2021), the projected number of things connected to the internet will be around 30.9 billion around the globe by the year 2025. In another prediction by McKinsey (Manyika et al., 2015), the economic value of IoT is expected to be USD 11.2 trillion by 2025. This rapid growth of IoT has been supported by advancements in technologies such as Cloud Computing, Big Data, and Artificial Intelligence. Another driving force is 5G technology which promises high-speed internet connectivity to handle the existing as well as new IoT networks (Painuly et al., 2020). However, with the huge number of devices connected to the Internet, a massive amount of data will be generated. Considering this, IoT will offer a huge opportunity for application organizers, Internet Service Providers, and product manufactures and will have an annual economic impact of around $2.69 trillion to $6.201 trillion by 2025 (Arne Holst, 2021). With advances in technologies, newly developed devices, and protocols, the IoT is leading today's digital transformation.

The success of the IoT has led to the introduction of the Web of Things (WoT) paradigm (Zeng et al. 2011; Guinard et al., 2011). At present, the web is the major medium of communication in today's Internet. Web services have been in use for decades and have proven to be very efficient in creating interoperable applications. Web services involving smart things with embedded web servers can be integrated into the existing web (Zeng et al. 2011). One of the advantages of the web of things is that they require less memory and no operating system support. However, there are a few issues to be addressed such as how to integrate the smart things into the existing web and how to abstract the integrated smart thing to web services (Guinard et al., 2011).

BACKGROUND

IoT has drawn significant attention not only from the industry but also from researchers across the globe. Several research articles have been published, describing the architecture and its applications in the last decade. There are a number of surveys and review papers that cover the different aspects of IoT technology (Atzori, et al., 2010; Yi & Liang, 2010; Gubbi et al.,2013; Ma, 2011; Kuyoro et al., 2015; Lee et al. 2017, Sethi & Sarangi, 2017). In addition, the authors also presented relevant applications of IoT. Although the emerging IoT has attracted a lot of demands, there are numerous issues to be addressed. There are many series of conferences which are themed to address these issues such as conferences organized by IEEE, ACM, and other societies including IFIP's CONFENIS, IEEE SMC International Conference on Enterprise Systems, International Conference on the Internet of Things etc.

IoT has become an active research area, with researchers exploring the different methods from various points of view to promote the development of IoT applications. Singh et al. (Singh et al., 2014), discussed the applications, services, visual aspects, and challenges for IoT. According to the authors, IoT is classified into three major versions: The things-oriented version, the Internet-oriented version, and the semantic-oriented version. The authors also discussed the challenges faced by WSNs for developing IoT communication networks. Atzori et al. (Atzor et al., 2010) in their survey gave an overview of the current state of the art on the IoT. They reviewed the enabling technologies and discussed different issues and open research challenges faced by the IoT domain until 2009 to help the researchers (Kassab & Darabkh, 2020). Some authors (Gubbi et al.,2013) presented a worldwide implementation of IoT based on Cloud computing. They also provided a roadmap of key technological developments in the context of IoT application domains. The paper also presented a Cloud implementation using the tool Aneka. The author discussed the need for convergence of WSN, the Internet, and distributed computing. These survey papers provide in-depth technical details and research challenges, which will help future researchers in this domain.

EVOLUTION OF IOT

The Internet has undergone a drastic evolution in the last three decades. The transition from IPv4 to IPv6 is evidence of this dynamic change. The concept of the IoT started to evolve from the first connected network called ARPANET developed by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense in 1969. A Coke vending machine at Carnegie Mellon University was the first internet-connected appliance to the university ARPANET in 1982. Later, in 1990 John Romkey connected a toaster to the internet which could be switched on and off over the internet. In 1984 and 1989 two major developments- the introduction of the Domain Name System and the World Wide Web took place (Serozhenko, 2017).

In 1993, the Trojan Room Coffee Pot was built in the University of Cambridge, London computer laboratory. Quentin Stafford-Fraser and Paul Jardetzky used a camera to monitor the pot levels and the image was put online for viewing on browsers. In 1995 another milestone was achieved when the Internet went commercial with Amazon and Echobay (Ebay). In 1997, Paul Saffo's prescient article was published on "Sensors: The Next Wave of Infotech Innovation'' (Singh et al., 2014).

The term IoT was first coined by Kevin Ashton, the executive director of the MIT Auto-ID Center. He described IoT as "uniquely identifiable interoperable connected objects with Radio-Frequency IDentification (RFID) technology". Neil Gershenfeld, Professor at MIT, also mentioned the concept of IoT in his book "When Things Start to Think '' in 1999 (Gershenfeld & Marder, 1999). In 2000, LG announced its first plan for 'connected appliances' – the Internet Refrigerator. Between the years 2003 to 2004, projects like Cooltown, Internet0, and the Disappearing Computer initiative started to implement some of the ideas of IoT (Serozhenko, 2017). The US Department of Defense in their SAVI program and Walmart in the commercial world started deploying RFID.

In 2005, the IoT reached the next level when the United Nations (UN) International Telecommunications Union (ITU) published its first report on the topic (Peña-López, 2005). The first IoT conference was held in March 2008 in Zurich. In the same year, the US National Intelligence Council listed IoT as one of the six disruptive civil technologies. As IPv4 address space wasn't sufficient to address the devices connected to the internet, in 2011 IPv6 was launched worldwide (Ziegler et al. 2012). In the same year, Cisco Internet Business Solutions Group released a white paper in which it asserted that IoT can be said to be born between 2008 and 2009.

In 2011 IoT was included in the Gartner Hype Cycle for Emerging technologies. In 2014 major developments took place in the area of IoT across the world. IoT home applications to control home lighting, doors, and temperature were developed. Also theme year Sigfox set up an Ultra Narrowband Wireless Data Network in the Bay Area of San Francisco and also Dublin, the capital city of Ireland, became the first IoT City. In 2017, many tech companies started to develop IoT applications and since then there has been a large increase in IoT devices each year ("The Rise of IoT: The History of the Internet of Things", 2020). The evolution of IoT is shown in Figure 1.

ARCHITECTURE LAYERS

The architecture model of the IoT describes the different components and the relationship between them. IoT should be capable of connecting a large number of things through the internet, which leads to more data traffic and the need for large data processors and storage. Due to this, IoT will face several challenges regarding Quality of Service (QoS), privacy, and security (Choudhary & Jain, 2016). To fulfil this criterion, IoT needs a flexible layered architecture. Currently, there is no widely accepted architecture model in the world (Kumar et al., 2018; Al-Fuqaha et al. 2015). From the literature, it is observed that different architectural models for IoT have been proposed which support different business interests. It is important to analyze these architectures to understand their strengths and weaknesses.

One of the basic IoT architectures proposed in the literature has three layers namely the perception layer, network layer, and application layer (Kumar & Mallick, 2018; Mashal et al. 2010; Said & Masud, 2013; Wu et al. 2010) as shown in figure 2. The proposed architecture is simple and easy to implement. The functionalities of each layer are described below:

- **Perception Layer:** The functionality of the perception layer is similar to the physical layer in the OSI model. It is a hardware layer that is concerned about overall device management (Al-Qaseemi et al. 2016). It identifies and collects information from the physical world, converts it into signals, and transfers it to the upper layer. This layer consists of different devices such as sensors, RFID, camera, GPS, and two-dimensional code equipment to collect the data such as temperature, vibrations, humidity, pH level, pressure, etc (Kraijak & Tuwanut, 2015).
- **Network Layer:** The network layer is responsible for transmitting and processing the information obtained from the perception layer (Choudhary & Jain, 2016). It helps to connect the smart things, network devices, and servers. The network layer includes a convergence network of communication

and Internet network, network management center, information center and intelligent processing center, etc (Kraijak & Tuwanut, 2015).

- **Application Layer:** The application layer is responsible for delivering application-specific services to the user. It defines various applications such as smart homes, smart cities, and smart health in which the IoT can be deployed (Kumar et al., 2018).

CASAGRAS, a project financed by the European Union (EU), proposed a 3-layer IoT architecture for IoT focusing on RFID, in support of IoT (EU FP7 Project CASAGRAS, 2009). The Consortium of CASAGRAS had predicted that the concept of IoT would go beyond RFID. The proposed architecture consisted of the Physical layer, Interrogator-Gateway Layer, Information Management, Application, and Enterprise Layer. The role of the Physical layer is the same as the perception layer of the three-layer architecture. Interrogator-Gateway Layer provides the interfaces between the things and between the interrogator and the information management systems. Information Management, Application, and Enterprise Layer provide interfacing with the interrogator-gateway layer and the information management layer. It also provides a functional platform for supporting applications and services.

The three-layer architecture of the IoT describes the functioning of IoT from the technical level. However, it is not sufficient to design a reliable solution considering the complexity of IoT. Also, research on IoT requires a focus on finer aspects. Hence there are many architectures proposed by the researchers. These include a 5-layer architecture for IoT proposed in the literature. Authors in (Wu et al., 2010) proposed a five-layer architecture based on Telecommunication Management Network layered architecture. The proposed model consists of five layers: perception, network, processing, application, and business layers as shown in figure 3. The role of the perception and application layers is the same as the architecture with three layers.

- The responsibility of the transport layer is to transfer the data from the perception layer to the processing layer and vice versa. In some IoT applications, data can be transferred to central information processing systems. It uses different network technologies ranging from Cellular networks GSM, 3G, and 4G, ZigBee, Z-wire, LAN, Bluetooth, RFID, and Wi-Fi to transfer the data (Lin et al., 2017). Also, the transport layer targets the use of IPv6 to address the devices used in an IoT application (Said & Masud, 2013).
- The processing layer, also known as the middleware layer, handles the data gathered by the perception layer. Its responsibility is to store, analyze, and process large amounts of data generated by devices (Mashal et al. 2010). It can manage and provide a diverse set of services to the lower layers. Since the amount of data involved is huge, it employs different technologies

such as databases, cloud computing, intelligent processing, and ubiquitous computing for information processing. Apart from this, the layer is also responsible for managing the service implemented by different objects (Said & Masud, 2013).

- The responsibility of the business layer is to manage the whole IoT system. This includes applications, business and profit models, and users' privacy (Al-Fuqaha et al. 2015; Singh et al., 2014). It uses the data received from the application layer to build business models, graphs, flow charts, etc., and uses Machine learning models to enhance operational optimization, mining insights, and business planning. It also manages all research related to IoT applications. Furthermore, metadata and reference data management, business rule management is also the responsibility of the business layer. It also monitors the operational health of lower layers (Weyrich & Ebert, 2016; Khan et al., 2012; Lin et al., 2017).

A Service-Oriented 5-layer Architecture for IoT (Wu et al. 2010; Spiess et al., 2009) is given in figure 4. The architecture has an Object layer, Object Abstraction, Service management, Service composition, and application layer. The function of the object layer is similar to the perception layer. The Object Abstraction Layer transfers the data produced by the Object layer to the Service Management layer through secure channels (Ray, 2018). Here various data transmission technologies are employed. Furthermore, it also handles cloud computing and data management processes (Haddad Pajouh et al., 2021). The Service Management layer pairs service with its requester based on addresses and names. This layer enables the IoT application programmers to work with heterogeneous objects without consideration to a specific hardware platform. Also, this layer processes received data, makes decisions, and delivers the required services (Al-Qaseemi et al. 2016; Chen & Jin, 2012; Tan & Wang, 2010). The service composition process permits the interaction between user requirements and smart objects of the IoT environment.

ROLE OF CLOUD COMPUTING

The IoT is a vision that enables a future connected world. The devices are connected and are capable of exchanging information to provide services to the users. In order to bring this vision to reality, several requirements must be considered. The most important issue is the dynamic management of the massive amount of data produced by these connected devices (Babu et al., 2015). The communication between the interconnected devices in IoT is going to generate enormous amounts of data. This is where cloud computing plays an important role to provide data storage and management support for IoT applications. Cloud and IoT have gone through a rapid and independent evolution. IoT and cloud computing are very different from each other, however, they complement each other. The integration of IoT and cloud will benefit in designing the applications.

Cloud computing allows resources, services, and data to be hosted on the Internet and to be available for use when needed (Biswas & Giaffreda, 2014). It makes the data and services universally accessible over the Internet. Cloud computing has been widely used over the last few years. The key characteristics of cloud computing are on-demand service provision, resource pooling, scalability, and elasticity. With cloud facilities, users can have visualization, machine learning, and data analytics options for wider sets of information (Botta et al., 2016). Moreover, cloud computing is location independent, and the users can access the cloud services from anywhere with an internet connection. These characteristics make cloud computing an integral part of IoT applications (Stergiou et al., 2018).

The Cloud in an IoT application can be used to store the data collected by the sensors and to process them intelligently in order to derive useful inferences from it. Due to the flexible and scalable nature of Cloud computing, it is capable of providing various services for IoT systems. These services include information storage options, software tools, and analytics, suitable platforms, and core infrastructure for the development (Cai et al., 2016). As a result, researchers have proposed Cloud-based IoT architecture and become popular in IoT systems (Kumar et al., 2018; Sethi & Sarangi, 2017).

In some of the cloud based IoT applications, the data processing is done in the cloud. This led to the IoT system having a cloud-centric architecture as shown in figure 5. In cloud-based IoT architectures, centralized control over the data is given and is achieved using cloud-based data processing systems. In such applications, the architecture keeps the cloud at the center, making the cloud to be in between the applications and network of things. (Kumar et al., 2018; Babu et al., 2015; Sethi & Sarangi, 2017; Aazam & Huh, 2014)

Despite the advantages of convergence of IoT and cloud in building IoT applications, the cloud still faces several challenges. The distance between the cloud and the end devices plays a crucial role for latency-sensitive applications such as disaster management, self-driving cars, and content delivery applications (Omoniwa et al., 2018). Such applications require high-bandwidth, ultra-low latency and computing should take place closer to the connected devices. Another issue is providing security to privacy-sensitive applications (Aazam & Huh, 2014). The massive amount of data generated by IoT applications will increase the load on the cloud. Fog computing addresses such issues by enabling the provisioning of resources and services closer to end devices. Fog works outside the cloud and at the edge of the network and is still possible to interact with the cloud. It is important to note that fog computing is a powerful complement to the cloud and not a substitute (Biswas & Giaffreda, 2014).

FOG COMPUTING

Fog computing is an emerging technology that enables data processing, analytics, and storage closer to the network edge. Fog computing acts as a bridge between the cloud and IoT devices and provides services like computing, storage, networking, and data management closer to IoT devices (Yousefpour et al., 2019). Fog is an intermediate layer composed of geo-distributed fog nodes. Fog handles the data processing in quite a different way compared to the cloud. In fog computing, the part of data processing and analytics is carried out at sensors and network gateways. Moreover, fog nodes filter out non-actionable data and send only useful data to the higher layer in the architecture. In this way, fog provides data protection and enables data processing in real-time and significantly reduces the bandwidth consumption in the backbone network (Bonomi et al., 2012).

There are clear differences between cloud and fog computing. Cloud computing provides high availability of computing resources and consumes more power (Bonomi et al., 2012). In contrast to this, fog computing provides moderate availability of computing resources and consumes less power. Cloud typically has large data centers and must be accessed through the network core. Whereas fog is designed to have small servers, gateways, and other networking devices which are connected closer to the IoT devices and can be accessed through connected devices from the edge of the network. One of the major differences is fog does not require continuous Internet connectivity. Fog-based services continue to work with low or no Internet connectivity. On the other hand, the cloud requires continuous internet connectivity in order to access the services.

In order to accommodate fog computing in IoT applications, the researchers have proposed IoT architecture based on Fog (Kumar et al., 2018). Fog-based IoT gateway as shown in figure 6 has the following layers: the physical layer, monitoring layer, pre-processing layer, storage layer, security layer, and transport layer. The physical layer contains IoT devices. The monitoring layer is responsible for monitoring power, available resources, required services, and responses. The pre-processing layer performs filtering, data processing, and analysis of the data generated by the sensors before sending it to the storage layers. The storage layer is used for temporary storage for providing functionality such as replication, distribution, and storage. The security layer helps in providing security and privacy to the data by applying encryption algorithms (Sethi & Sarangi, 2017).

Despite several benefits of fog computing, there are a few research challenges to address. Fog computing is still in an early stage and an open research area. Currently, the fog nodes are assumed to be fixed. There is not much support for mobile fog computing. More research needs to be done on resources allocations in the cloud and fog layers maintaining the performance of fog nodes compared to the cloud (Abi Sen & Yamin, 2020; Yousefpour et al., 2019).

5G TECHNOLOGY

The current 4G LTE generation is a completely all IP-based system. However, the amount of data generated by IoT devices will put pressure on the existing LTE architecture (Chettri & Bera, 2019). Moreover, LTE will not be sufficient to meet the requirements of IoT applications such as ultra-reliable, secure, low latency, high data rate, and high bandwidth network. In order to address these issues, 5G is considered the most promising technology (Shafique et al., 2020).

5G and IoT are evolving rapidly on a global level. The International Telecommunication Union (ITU) defined the vision for 5G as "the connectivity for anything" which means 5G will connect everything around us with a fast and highly reliable, and low latency network. It is expected that by 2023 5G-IoT implementation will begin and will become the preferred IoT network (Painuly et al., 2020). In order to support IoT, several features and network-enabling technologies have been proposed in 5G (Shafique et al., 2020; Gupta & Jha, 2015).

1. **Software-defined wireless sensor networking (SD-WSN)** will blend SDN inside the WSN. This will provide a centralized mechanism to program the entire network.
2. **Network Function Virtualization (NFV)** enables network virtualization by implementing network functions as software packages. The NFV aims to provide a scalable and flexible network for 5G-IoT applications. It enables customized network slicing over distributed clouds and creates programmable networks for IoT applications.
3. **Cognitive Radios (CRs)** address the issue of scarcity of spectrum. It can be defined as "a radio that can change its transmitter parameters based on the interaction with the environment in which it operates''
4. **mmWaves** enhances data rates in 5G. Massive MIMO and beamforming techniques used in 5G efficiently uses the spectrum.

The QoS parameters for IoT applications are dependent on the use case and can have varying requirements in terms of throughput, delay, and jitter. For example, Home automation applications are not delay-sensitive whereas Artificial Intelligent based self-driving cars are very sensitive to delay. Hence, in 5G three main categories of use cases are defined by 3GPP (Fettweis, 2016).

- **Enhanced Mobile Broadband (eMBB)** will support data-intensive applications which require high bandwidth. These applications include high-definition video transmission, gaming applications, and other such use cases.
- **Massive Machine Type Communication (MMTC)** will support the IoT use cases which are low-cost, low-energy devices, and generate small data volumes.
- **Ultra-Reliable and Low Latency Communications (URLLC)** will support delay-sensitive applications such as self-driving cars which require high reliability, low latency.

Many research articles have been published in the area of 5G-IoT. A detailed survey of the 5G network architecture is provided in (Yassein et al., 2017). The authors discussed emerging technologies such as interference management, spectrum sharing with the help of cognitive radio, Software Defined Networks, etc. An overview of characteristics and applications of 5G IoT are presented in (Fettweis, 2016). The research challenges and applications of 5G IoT are discussed in (Painuly et al., 2020; Chettri & Bera, 2019; Javaid et al., 2018). A survey of key enabling technologies and emerging use cases of 5G-IoT are presented in (Shafique et al., 2020). The authors also discussed ongoing 5G initiatives and challenges in the implementation of 5G-IoT. Although the features provided by 5G satisfy the requirements of the future IoT, there are still several research challenges that need to be addressed. These include the architecture of 5G-IoT, and security issues, etc (Gupta & Jha, 2015).

APPLICATIONS OF IOT

IoT has applications in different areas including Home automation, healthcare, transport, supply chain, environment and agriculture, manufacturing and industry, traffic management, and many more. According to the data from IoT - analytics (Knud, 2018) collected in 2018 from the USA most of the IoT projects identified are Smart City followed by industrial settings projects and Connected Building IoT projects. Similarly, according to Fortune Business Insights report on IoT (Fortune Business Insights, 2021) the market was $381.30 billion in 2021 and forecasted to reach $1,854.76 billion in 2028. According to this report, the market stood at USD 250.72 billion in 2019.

As we all witnessed, in 2019 COVID-19 pandemic resulted in a severe economic downfall of industries and businesses. However, the restrictions on the movement of people resulted in higher demand for IoT solutions, especially in the healthcare domain. People started using IoT techniques to detect the COVID-19 infected people and for contact tracing. Moreover, it helped government officials to efficiently monitor the areas with high infection rates. These resulted in the positive growth of the market amid the pandemic.

In India currently, there is increased adoption of IoT in areas such as home automation, customer engagement, healthcare, virtual conferencing, etc. In this section, a few IoT applications are discussed along with the recently published works.

Smart Home System

One of the most practical and popular applications of IoT is a smart home system. A sample home automation system with connected devices is shown in figure 7. Smart homes have the technology to allow all the home appliances to be controlled automatically and can be controlled remotely through the internet. It provides both convenience and home security to the user. There are different levels at which the concept of IoT can be applied to smart homes. It could be automatic illumination systems, connected surveillance systems or advanced locking systems, or a combination of some of them. Smart homes require 3 things: an internal network, intelligent control, and home automation (Jie et al., 2013). The internal network is used for the communication between sensors and actuators to provide services to humans. The intelligent control is a gateway and to be managed or be monitored by internet servers. Home automation consists of computing services that are applications run by users (Yamazaki, 2006).

Nowadays homeowners are becoming more sensitive towards energy consumption, and security. As a result, the trend of home automation slowly began to pace in India. Consequently, many companies came up with home automation products specifically designed for Indian homes such as smart lighting, thermostat sensors, smart TV, and more. Some of the popular companies which produce smart home automation products include Schneider Electric, Cubical Labs, Buildtrack, Zemote, Legrand, Philips, Oakter, and SharpNode. Among these, Oakter and SharpNode are Indian start-up companies. According to Statista (Arne Holst, 2021), the Indian smart homemaker market is expected to touch USD 6 billion by 2022. Globally, this number is expected to reach USD 53.4 billion by 2022.

Although the Smart home concept became popular recently, the idea had started way back in the 1970s. In the 1990s, due to development in technologies such as wired and wireless home networking, sensor networks, networked appliances, researchers started smart home projects. Authors (Kidd et al., 1999) proposed the Aware Home project to create a living laboratory for research in ubiquitous computing for everyday activities. They implemented some parts of proposed systems including human position tracking through ultrasonic sensors, RF technology, and video recognition through floor sensors and vision techniques.

Stephen S. Intille in ((Intille, 2002) from the School of Architecture and Planning, MIT, published an article on Designing a Home of the Future which emphasized 3 parameters namely the point of decision, the point of behavior, and the point of consequence for a smart home. In 2003, Housing Learning & Improvement Network published a smart home definition offered by Intertek. According to Intertek, a smart home is “a dwelling incorporating a communications network that connects the key electrical appliances and services, and allows them to be remotely controlled, monitored or accessed”.

Jie, Yin, et al in 2013 (Jie, Yin, et al., 2013) proposed the idea of applying IoT technologies to smart home systems. The authors proposed a few agents to communicate with appliances through RFID tags. A survey on smart homes (Al-Ali et al., 2004) published in 2004 provides definition, research status, projects, and some of the research challenges with respect to smart home applications. The authors also described some home appliances and projects to make a user’s life more comfortable. Gaikwad et. al in 2015 (Gaikwad et. al, 2015) discussed challenges and some solutions for a smart home system using loT. Kang Bing et al proposed layered architecture for Smart Home System based on IoT in (Bing, et al., 2011). The proposed architecture was divided into three layers: application layer, network layer, and sensing layer. The authors used SAMSUNG S3C2440A, a type of ARM microcontroller, for data collection and data processing and Zigbee standard for transferring the collected data to the network layer.

There are many research problems and issues to be addressed before building a Smart Home system. One of the main challenges is providing security. A proper authentication method is required on the server side. Otherwise, an attacker can get access to the victim’s home. Secondly, maintaining the confidentiality of the user’s data is very important.

Agriculture

IoT is gaining popularity in the agriculture field as well. IoT-enabled agriculture can help farmers to make informed decisions and the desired outcome. Agriculture is the primary source of food and the main source of income in many countries. Particularly in India, 70% of the population is dependent on agriculture and contributes approximately 18% to the country’s GDP (Das et al., 2019). However, with deforestation and change in weather conditions, the agriculture sector is facing several challenges. The emergence of IoT has brought a great revolution in agriculture by adapting "Smart farming" applications like soil moisture monitoring, water level monitoring, and helping farmers to improve crop yields.

The term smart farming refers to modern farming management with the application of IoT technology to increase productivity in agriculture (Muangprathub et al., 2019). IoT-based smart farming consists of sensor devices, processing modules to process the collected data, connectivity, gateway, and cloud (Doshi et al., 2019). IoT solutions can help farmers to monitor crops, to control irrigation remotely, and to detect soil properties, detect and monitor pests, etc. In India, many start-up companies have come up with IoT-based products to assist farmers in taking farming-related decisions. Some of them are listed below.

- **Aquaconnect** aims to help shrimp and fish farmers by using artificial intelligence and remote-sensing technologies to monitor the water quality and feeding results.
- **BharatAgri** developed products that provide personalized farming suggestions regarding irrigation and fertilization to the farmers by collecting data and applying algorithms to provide suggestions.
- **Intello** Labs developed a food assessment product using AI-based image technology to help farmers, retailers, and other supply chain companies to control food quality.
- **Agdhi** developed a product to detect seed defects, diagnose crop diseases, and build farmer networks. They used AI and computer vision technology to find problematic seeds or crops.

From the research perspective, a significant amount of work has been done on applying IoT technology in the agriculture area. Many articles have been published in the area of IoT-based smart farming. Raju et. al (Das et al., 2019) provided a complete survey on the application of IoT in agriculture, emerging wireless technologies of IoT. The survey provides details of different crop types, climatic conditions required, and agriculture disease identification. The authors reviewed the existing work in the field of IoT in agriculture and provided future research challenges. Farooq et al., (Farooq et al., 2019) presented different components and technologies involved in developing IoT-based smart farming applications. Furthermore, the authors provided a comprehensive discussion on network technologies and other relevant technologies such as cloud computing, big data storage, and analytics and security issues in agriculture IoT.

Muangprathub et al. (Muangprathub et al., 2019) developed an optimal watering system based on WSN for agricultural crops. The authors developed a control system consisting of three components: hardware (Soil moisture sensors), web application, and mobile application. Data mining techniques were applied to analyze the data collected from the soil moisture sensor and predict suitable temperature, soil moisture, and humidity, for crop growth. Krushna Das et al. (Das et al., 2019) proposed a smart agriculture system in India using the IoT to minimize crop loss during harvest or post-harvest.

In the field of smart farming, the IoT plays a very important role. IoT-based solutions will help the farmers to automatically maintain and monitor agricultural farms with minimal human involvement. However, there are a few research challenges which need to be addressed. Firstly, the implementation of smart farming applications requires a large number of sensors to be deployed in agriculture farms for data acquisition. Most of these applications use the unlicensed spectrum for data transmission and may create interference (Das et al., 2019). Secondly, providing the physical safety of the deployed sensors is necessary to secure the devices from unauthorized users. Thirdly, most of the farmers are not trained to handle IoT devices (Friha et al., 2021). The lack of knowledge of IoT and its applications in farmers is slowing down the growth of IoT in agriculture.

Healthcare

The experience with the COVID-19 pandemic has shown the world the need for robust health infrastructure. The emergence of IoT has enormous potential and benefits in the healthcare system in enabling healthcare organizations to focus more on service and improved patient outcomes. IoT can help healthcare professionals to monitor their patient's health conditions and also patients can monitor themselves. With the use of wearable devices and smart sensors, the healthcare systems are shifting towards IoT-based applications to provide better healthcare facilities. The most common applications of IoT in healthcare include remote patient monitoring, Glucose monitoring, Heart rate monitoring, wearable fitness band, and many more. Moreover, IoT devices tagged with sensors can also be used to track the location of medical equipment during emergencies and can provide real-time location information of medical equipment (Selvaraj & Sundaravaradhan, 2020).

It is obvious to admit that IoT enables better healthcare environments and reduces the cost for treatment, and improves collaboration with health practitioners and patients (Onasanya & Elshakankiri, 2019). Recent advancements in IoT technology have opened many opportunities for developing IoT-based applications for healthcare systems. Many start-up companies in India focus on developing IoT-based healthcare applications/products. Some of them are listed below:

- **Spectral Insights** created a platform that provides innovative imaging, advanced analytics, and digital microscopy for hospitals, pharma Research and Development, and clinical laboratories.

- **Forus Health** developed technology solutions to make affordable access to eye care. Their first product called 3nethra classic is a portable and compact non-mydriatic fundus camera that helps to identify common eye problems such as glaucoma, diabetic retinopathy, cataract, etc. Also, it is integrated with a cloud-based telemedicine platform that enables remote diagnosis.
- **Cardiac Design Labs** offer diagnosis and cardiac monitoring by deploying intelligent systems that give automatic remote reporting. The company has created a wearable device named MIRCaM (Mobile Intelligent Remote Cardiac Monitor) which provides real-time cardiac monitoring and diagnosis in remote settings.
- **Bagmo Pvt Ltd.** company created a blood bag monitoring device to monitor the temperature of blood bags during storage and transportation. Also, it helps to reduce wastage at blood collection centers by connecting an RFID card to each bag and using a cloud platform.
- **Prantae Solutions** develops devices and diagnostic solutions for pregnancy-related healthcare.
- **Waferchips Techno Solutions** has developed a wearable Electrocardiography (ECG) device called Biocalculus. The device uses artificial intelligence (AI) to generate a clinically actionable report for further diagnosis and treatment.
- **Janitri Innovations** developed a product Keyar, a non-invasive cardiotocography (CTG) device, to monitor the heart rate of a baby in the mother's womb. The device also tracks uterine contractions of pregnant women. It is portable, runs on ordinary batteries, and can be used in remote areas.
- **EzeRx** developed a product called AJO (anemia, jaundice, and oxygen saturation), to test for anemia, liver, and lung-related medical problems without any blood work.

Apart from these startup companies, many researchers have made significant contributions in developing technologies that support IoT-based healthcare applications. The Selvaraj & Sundaravaradhan (Selvaraj & Sundaravaradhan, 2020) analyzed the research articles published in the domain of IoT-based healthcare systems and reviewed data management methods using cloud facilities. Kumar & Gandhi (Kumar & Gandhi, 2018) proposed an IoT architecture to detect heart diseases in an early stage using machine learning algorithms. The proposed 3-tier architecture has sensors for collecting data from wearable devices. The system uses a cloud for storing the data and a regression-based prediction model for predicting heart diseases. Adeniyi Onasanya and Maher Elshakankiri proposed a smart healthcare system for cancer patients (Onasanya & Elshakankiri, 2019). The proposed system architecture has different layers for Service, Data center, Cancer care, Hospital, and

Security management. The authors also proposed the implementation of the cancer care services along with business analytics. The system enables decision-making; data transmission; and reporting. The authors also provided a detailed comparison of the proposed system with the existing systems.

Authors (Kandil & El-Deeb, 2016) proposed the Cloud-IoT healthcare system to create a network consisting of healthcare stakeholders: patients and their family members, healthcare professionals, Pharmacists, hospitals, etc. The proposed system has various applications such as an e-prescribing module, electronic health record, clinical decision system, and so on. However, the proposed system has not considered the security threats. Also, the security model is not provided. Mohammed Al-Khawaja et al (Al-Khawaja et al., 2018) proposed a fog-based IoT healthcare architecture that consists of three layers: things, fog nodes, and a cloud data center. The proposed architecture provides collaboration among fog nodes with optimal resource management and job allocation. Parthsarathy and Vivekandan (Parthsarathy & Vivekandan, 2020) proposed an IoT-based design for monitoring a patient who is affected by arthritis. The authors used wearable sensor gadgets and Uric Acid sensors to build the health monitoring framework. Anjali Yeole in the survey article in (Yeole & Kalbande, 2016), studied the use of various IoT devices (sensors) for childcare and chronic diseases. The author provided a thorough comparison of different IoT devices with respect to the battery life, users, and many other parameters.

At present, the global medical problem is a real concern. Although there are a lot of advantages of using IoT in providing better healthcare facilities, there are several research challenges that need to be addressed. One of the major challenges is providing security to the patient data and maintaining confidentiality. Wearable devices are becoming part of humans' daily activities. These devices monitor and collect all the user information and may collect sensitive information without user consent. Hence there is a possibility of violating the user's privacy. Also, hackers can use these sensitive data for wrong purposes. Hence more research on providing security and, privacy to the user data needs to be addressed. IoT applications may use a diverse set of sensors and other devices which are manufactured by different manufacturers. The real challenge is the integration of heterogeneous devices, manufacturers, and communication protocols. Considering the present global pandemic situation, there is a need for IoT-based smart disease surveillance systems for the early detection of infectious threats.

CONCLUSION

Internet of Things is a future Internet as it permits the things to communicate directly and perform various tasks without much human involvement. IoT has applications in many fields such as home automation, agriculture, healthcare, traffic management, industry automation etc. In this chapter the author provided an overview of the IoT with emphasis on evolution, enabling Architecture, and applications. To understand the concept of IoT, chapter provides the insights into the different architecture of IoT. A brief overview of the architecture layers proposed by different researchers includes the basic three-layer, five-layer, SOA based, Cloud and fog-based architectures. The research challenges associated with these layers are also presented. From this study, it can be concluded that as the number of layers in the architecture increases, it is more complex to integrate IoT applications with the practical environment. The authors have discussed three main applications of IoT - Home automation, agriculture, and healthcare and the recent work done in these areas. This chapter would help the researchers who are working in the area of IoT to gain the basic understanding of the research area.

REFERENCES

Aazam, M., & Huh, E. N. (2014, August). Fog computing and smart gateway based communication for cloud of things. In *2014 International Conference on Future Internet of Things and Cloud* (pp. 464-470). IEEE. 10.1109/FiCloud.2014.83

Abi Sen, A. A., & Yamin, M. (2020). Advantages of using fog in IoT applications. *International Journal of Information Technology*, 1-9.

Al-Ali, A. R., & Al-Rousan, M. (2004). Java-based home automation system. *IEEE Transactions on Consumer Electronics*, *50*(2), 498–504. doi:10.1109/TCE.2004.1309414

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. doi:10.1109/COMST.2015.2444095

Al-Khafajiy, M., Webster, L., Baker, T., & Waraich, A. (2018, June). Towards fog driven IoT healthcare: challenges and framework of fog computing in healthcare. In *Proceedings of the 2nd international conference on future networks and distributed systems* (pp. 1-7). 10.1145/3231053.3231062

Al-Qaseemi, S. A., Almulhim, H. A., Almulhim, M. F., & Chaudhry, S. R. (2016, December). IoT architecture challenges and issues: Lack of standardization. In 2016 Future technologies conference (FTC) (pp. 731-738). IEEE.

Arne Holst. (2021, Oct 19). *Number of IoT connected devices worldwide 2019-2030*. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787–2805. doi:10.1016/j.comnet.2010.05.010

Babu, S. M., Lakshmi, A. J., & Rao, B. T. (2015, April). A study on cloud based Internet of Things: CloudIoT. In 2015 global conference on communication technologies (GCCT) (pp. 60-65). IEEE.

Bing, K., Fu, L., Zhuo, Y., & Yanlei, L. (2011, July). Design of an Internet of Things-based smart home system. In *2011 2nd International Conference on Intelligent Control and Information Processing* (Vol. 2, pp. 921-924). IEEE. 10.1109/ICICIP.2011.6008384

Biswas, A. R., & Giaffreda, R. (2014, March). IoT and cloud convergence: Opportunities and challenges. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 375-376). IEEE.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16). 10.1145/2342509.2342513

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, *56*, 684–700. doi:10.1016/j.future.2015.09.021

Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2016). IoT-based big data storage systems in cloud computing: Perspectives and challenges. *IEEE Internet of Things Journal*, *4*(1), 75–87. doi:10.1109/JIOT.2016.2619369

Chen, X. Y., & Jin, Z. G. (2012). Research on key technology and applications for internet of things. *Physics Procedia*, *33*, 561–566. doi:10.1016/j.phpro.2012.05.104

Chettri, L., & Bera, R. (2019). A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal*, *7*(1), 16–32. doi:10.1109/JIOT.2019.2948888

Choudhary, G., & Jain, A. K. (2016, December). Internet of Things: A survey on architecture, technologies, protocols and challenges. In *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* (pp. 1-8). IEEE. 10.1109/ICRAIE.2016.7939537

Das, R. K., Panda, M., & Dash, S. S. (2019). Smart agriculture system in India using internet of things. In *Soft computing in data analytics* (pp. 247–255). Springer. doi:10.1007/978-981-13-0514-6_25

De Donno, M., Tange, K., & Dragoni, N. (2019). Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 150936–150948. doi:10.1109/ACCESS.2019.2947652

Doshi, J., Patel, T., & Kumar Bharti, S. (2019). Smart Farming using IoT, a solution for optimally monitoring farming conditions. *Procedia Computer Science*, *160*, 746–751. doi:10.1016/j.procs.2019.11.016

EU FP7 Project CASAGRAS, (2009). *CASAGRAS Final Report: RFID and the Inclusive Model for the Internet of Things*. Author.

Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 156237–156271. doi:10.1109/ACCESS.2019.2949703

Fettweis, G. P. (2016, September). 5G and the future of IoT. In *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference* (pp. 21-24). IEEE.

Fortune Business Insights. (2021). *Internet of Things (IoT) Market Size, Share & COVID-19 Impact Analysis, By Component (Platform, Solution & Services), By End-Use Industry (BFSI, Retail, Government, Healthcare, Manufacturing, Agriculture, Sustainable Energy, Transportation, IT & Telecom, Others), and Regional Forecast, 2021-2028*. https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307

Friha, O., Ferrag, M. A., Shu, L., Maglaras, L. A., & Wang, X. (2021). Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies. *IEEE CAA J. Autom. Sinica*, *8*(4), 718–752. doi:10.1109/JAS.2021.1003925

Gaikwad, P. P., Gabhane, J. P., & Golait, S. S. (2015, April). A survey based on Smart Homes system using Internet-of-Things. In *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)* (pp. 330-335). IEEE. 10.1109/ICCPEIC.2015.7259486

Gershenfeld, N., & Marder, M. (1999). When Things Start to Think and the Nature of Matheinatical Modeling. *Physics Today*, *52*(10), 75. doi:10.1063/1.882867

Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). *Cyber-Physical Systems and Internet of Things, Special Publication (NIST SP)*. National Institute of Standards and Technology. [online], doi:10.6028/NIST.SP.1900-202

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Guinard, D., Trifa, V., Mattern, F., & Wilde, E. (2011). From the internet of things to the web of things: Resource-oriented architecture and best practices. In *Architecting the Internet of things* (pp. 97–129). Springer. doi:10.1007/978-3-642-19157-2_5

Gupta, A., & Jha, R. K. (2015). A Survey of 5G Network: Architecture and Emerging Technologies. *IEEE Access: Practical Innovations, Open Solutions*, *3*, 1206–1232. doi:10.1109/ACCESS.2015.2461602

HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129. doi:10.1016/j.iot.2019.100129

Intille, S. S. (2002). Designing a home of the future. *IEEE Pervasive Computing*, *1*(2), 76–82. doi:10.1109/MPRV.2002.1012340

Javaid, N., Sher, A., Nasir, H., & Guizani, N. (2018). Intelligence in IoT-based 5G networks: Opportunities and challenges. *IEEE Communications Magazine*, *56*(10), 94–100. doi:10.1109/MCOM.2018.1800036

Jie, Y., Pei, J. Y., Jun, L., Yun, G., & Wei, X. (2013, June). Smart home system based on iot technologies. In *2013 International conference on computational and information sciences* (pp. 1789-1791). IEEE. 10.1109/ICCIS.2013.468

Jung, M., Hajdarevic, E., Kastner, W., & Jara, A. (2014, March). Short paper: A scripting-free control logic editor for the Internet of Things. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 193-194). IEEE.

Kandil, A., & El-Deeb, H. (2016, January). Exploration of application migration to cloud environment. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 109-114). IEEE. doi:10.1109/CONFLUENCE.2016.7508097

Kassab, W. A., & Darabkh, K. A. (2020). A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, *163*, 102663. doi:10.1016/j.jnca.2020.102663

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *2012 10th international conference on frontiers of information technology* (pp. 257-260). IEEE. 10.1109/FIT.2012.53

Kidd, C. D., Orr, R., Abowd, G. D., Atkeson, C. G., Essa, I. A., MacIntyre, B., ... Newstetter, W. (1999, October). The aware home: A living laboratory for ubiquitous computing research. In *International workshop on cooperative buildings* (pp. 191-198). Springer. 10.1007/10705432_17

Knud Lasse Lueth. (2018, February 22). *The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects*. https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/

Kraijak, S., & Tuwanut, P. (2015, September). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. In *11th international conference on wireless communications, networking and mobile computing (WiCOM 2015)* (pp. 1-6). IET. 10.1049/cp.2015.0714

Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. *Procedia Computer Science*, *132*, 109–117. doi:10.1016/j.procs.2018.05.170

Kumar, P. M., & Gandhi, U. D. (2018). A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. *Computers & Electrical Engineering*, *65*, 222–235. doi:10.1016/j.compeleceng.2017.09.001

Kumar, R. P., & Smys, S. (2018, January). A novel report on architecture, protocols and applications in Internet of Things (IoT). In *2018 2nd International Conference on Inventive Systems and control (ICISC)* (pp. 1156-1161). IEEE.

Kuyoro, S., Osisanwo, F., & Akinsowon, O. (2015, March). Internet of things (IoT): an overview. In *Proc. of the 3rd International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM)* (pp. 23-24). Academic Press.

Lee, S. K., Bae, M., & Kim, H. (2017). Future of IoT networks: A survey. *Applied Sciences (Basel, Switzerland)*, *7*(10), 1072. doi:10.3390/app7101072

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 Journal*, *4*(5), 1125–1142. doi:10.1109/JIOT.2017.2683200

Ma, H. D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer Science and Technology*, *26*(6), 919–924. doi:10.100711390-011-1189-5

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *Unlocking the potential of the Internet of Things*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, *28*, 68–90. doi:10.1016/j.adhoc.2014.12.006

Muangprathub, J., Boonnam, N., Kajornkasirat, S., Lekbangpong, N., Wanichsombat, A., & Nillaor, P. (2019). IoT and agriculture data analysis for smart farm. *Computers and Electronics in Agriculture*, *156*, 467–474. doi:10.1016/j.compag.2018.12.011

Omoniwa, B., Hussain, R., Javed, M. A., Bouk, S. H., & Malik, S. A. (2018). Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. *IEEE Internet of Things Journal*, *6*(3), 4118–4149. doi:10.1109/JIOT.2018.2875544

Onasanya, A., & Elshakankiri, M. (2019). Smart integrated IoT healthcare system for cancer care. *Wireless Networks*, 1–16.

Painuly, S., Kohli, P., Matta, P., & Sharma, S. (2020, December). Advance applications and future challenges of 5G IoT. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 1381-1384). IEEE.

Parthasarathy, P., & Vivekanandan, S. (2020). A typical IoT architecture-based regular monitoring of arthritis disease using time wrapping algorithm. *International Journal of Computers and Applications*, *42*(3), 222–232. doi:10.1080/1206212X.2018.1457471

Peña-López, I. (2005). *ITU Internet report 2005: the internet of things*. https://www.itu.int/osg/spu/publications/internetofthings/

Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences*, *30*(3), 291–319. doi:10.1016/j.jksuci.2016.10.003

Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. *International Journal of Computer Networks*, *5*(1), 1–17.

Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: A systematic review. *SN Applied Sciences*, *2*(1), 1–8. doi:10.100742452-019-1925-y

Serozhenko, M. (2017, Jun 15). *Brief history of the internet of things*. https://medium.com/mqtt-buddy/brief-history-of-the-internet-of-things-f00043ae17b5

Sethi, P., & Sarangi, S. R. (2017). Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*, 2017. doi:10.1155/2017/9324035

Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 23022–23040. doi:10.1109/ACCESS.2020.2970118

Simoniot. (2020, Nov 20). *The Rise of IoT: The History of the Internet of Things*. https://www.simoniot.com/history-of-iot/

Singh, D., Tripathi, G., & Jara, A. J. (2014, March). A survey of Internet-of-Things: Future vision, architecture, challenges and services. In 2014 IEEE world forum on Internet of Things (WF-IoT) (pp. 287-292). IEEE.

Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., De Souza, L. M. S., & Trifa, V. (2009, July). *SOA-based integration of the internet of things in enterprise services. In 2009 IEEE international conference on web services*. IEEE.

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964–975. doi:10.1016/j.future.2016.11.031

Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-376). IEEE.

Weyrich, M., & Ebert, C. (2015). Reference architectures for the internet of things. *IEEE Software*, *33*(1), 112–116. doi:10.1109/MS.2016.20

Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-484). IEEE.

Yamazaki, T. (2006, November). Beyond the smart home. In *2006 International Conference on Hybrid Information Technology* (Vol. 2, pp. 350-355). IEEE. 10.1109/ICHIT.2006.253633

Yassein, M. B., Aljawarneh, S., & Al-Sadi, A. (2017, November). Challenges and features of IoT communications in 5G networks. In *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)* (pp. 1-5). IEEE. 10.1109/ICECTA.2017.8251989

Yeole, A. S., & Kalbande, D. R. (2016, March). Use of Internet of Things (IoT) in healthcare: A survey. In *Proceedings of the ACM Symposium on Women in Research 2016* (pp. 71-76). 10.1145/2909067.2909079

Yi, D. L., & Liang, D. (2010). A survey of the internet of things. *Proc. of ICEBI.*

Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., & Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture*, *98*, 289–330. doi:10.1016/j.sysarc.2019.02.009

Zeng, D., Guo, S., & Cheng, Z. (2011). The web of things: A survey. *Journal of Communication*, *6*(6), 424–438.

Ziegler, S., Skarmeta, A., Kirstein, P., & Ladid, L. (2015, December). Evaluation and recommendations on IPv6 for the Internet of Things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 548-552). IEEE. 10.1109/WF-IoT.2015.7389113

ADDITIONAL READING

Chase, J. (2013). The evolution of the internet of things. *Texas Instruments*, *1*, 1–7.

De Michele, R., & Furini, M. (2019, September). IOT healthcare: Benefits, issues and challenges. In *Proceedings of the 5th EAI international conference on smart objects and technologies for social good* (pp. 160-164). 10.1145/3342428.3342693

Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, *10*, 1–9. doi:10.1016/j.jii.2018.01.005

Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(05), 164–173. doi:10.4236/jcc.2015.35021

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative*, *1*(1), 1–86.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. doi:10.1016/j.adhoc.2012.02.016

Nguyen, H. H., Mirza, F., Naeem, M. A., & Nguyen, M. (2017, April). A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback. In *2017 IEEE 21st International conference on computer supported cooperative work in design (CSCWD)* (pp. 257-262). IEEE. 10.1109/CSCWD.2017.8066704

Raju, K. L., & Vijayaraghavan, V. (2020). IoT technologies in agricultural environment: A survey. *Wireless Personal Communications*, *113*(4), 2415–2446. doi:10.100711277-020-07334-x

Sonune, S., Kalbande, D., Yeole, A., & Oak, S. (2017, June). Issues in IoT healthcare platforms: A critical study and review. In *2017 International Conference on Intelligent Computing and Control (I2C2)* (pp. 1-5). IEEE. 10.1109/I2C2.2017.8321898

KEY TERMS AND DEFINITIONS

5G: It is the fifth Generation of wireless access networks.

Cyber-Physical System (CPS): An integration of computation and physical processes, in which operations are monitored, coordinated, controlled and integrated by a computing and communication core.

Global Positioning System (GPS): A satellite-based navigation system that provides location, velocity and time synchronization to the users.

IPv6 (Internet Protocol Version 6): A 128-bit long network layer protocol that is used to uniquely address the devices connected to the network.

Long-Term Evolution (LTE): A wireless access network technology that is considered the fourth-generation wireless system.

Radio Frequency Identification (RFID): The wireless system to transfer data which uses radio frequency waves to transfer data.

Wireless Sensor Networks (WSN): A network composed of a large number of sensor nodes, which are densely deployed to monitor the system, physical or environmental conditions.

Zigbee: Is a wireless access technology which operates on the IEEE 802.15.4 standard and developed to address the needs of low-cost, low-power wireless IoT networks.

APPENDIX

Figure 1.

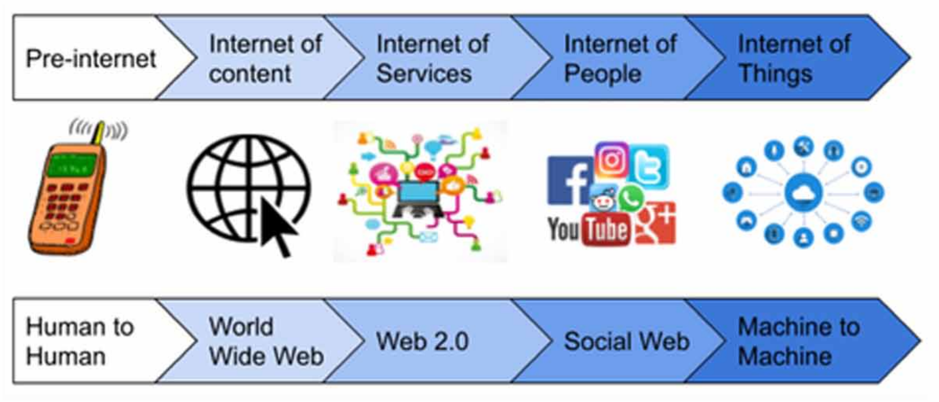


Figure 2.

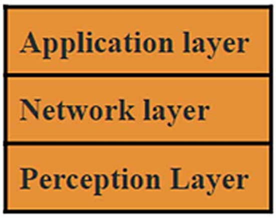


Figure 3.

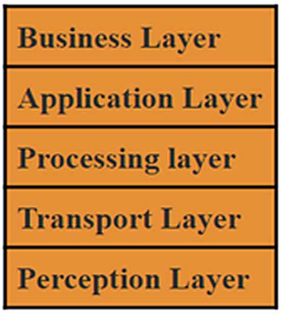


Figure 4.

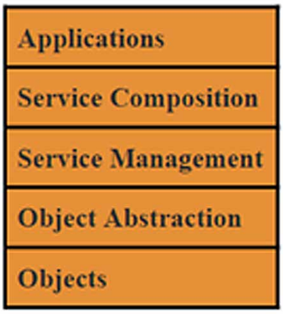


Figure 5.

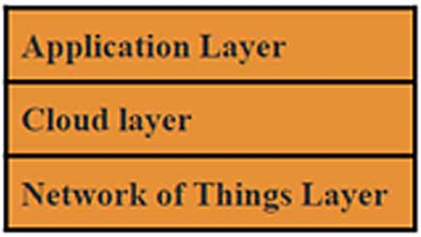


Figure 6.

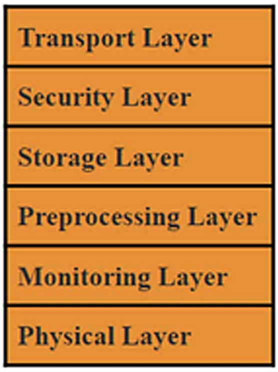
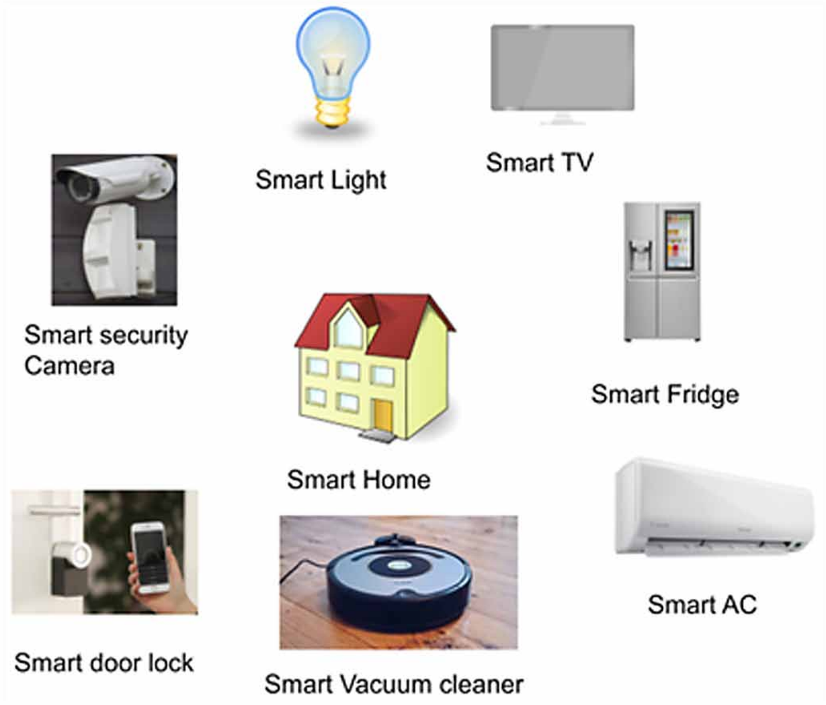


Figure 7.


Smart Light
Smart TV
Smart security Camera
Smart Fridge
Smart Home
Smart AC
Smart door lock
Smart Vacuum cleaner

Chapter 2
AssessLIFE Software for Automation of Asset Degradation to Estimate Asset Life and Degradation Drivers

Emenike Raymond Obi
RaySoft AssetAnalytics, Canada

Augustine O. Nwajana
https://orcid.org/0000-0001-6591-5269
University of Greenwich, UK

ABSTRACT

The AssessLIFE software is a solution platform that analyzes and reveals if industrial physical assets made of metals, alloys, and welds can survive their exposure or ambient conditions. The software also reveals when time-dependent premature failure is likely to occur. The software can generate great financial and safety benefits for all stakeholders. Furthermore, the AssessLIFE software aims to provide asset information for better financial and technical decision-making by managers, engineers, legal teams, insurance teams, fabricators, and inspectors.

DOI: 10.4018/978-1-6684-3855-8.ch002

INTRODUCTION

Environmental Impact of Alloy Degradation

"The three main global challenges for the twenty-first century are energy, water, and air – that is, sufficient energy to ensure a reasonable standard of living, clean water to drink, and clean air to breathe. The ability to manage corrosion is a central part of using materials effectively and efficiently to meet these challenges" (Revie & Uhlig, 2008, p. xvii). AssessLIFE Software ties aptly into providing solutions to one of the biggest challenges facing humankind in the modern world, namely the effective and efficient use of generated energy and the reduction of greenhouse gases released into the atmosphere. AssessLIFE Software provides a means to select the right alloys for the right industrial applications to ensure that the alloys employed in industrial settings globally for the production of goods and services attain reasonable service-lives or lifespans and minimize the high risks of premature asset failures. Alloy premature failures typically involve the replacement of the failed assets with assets made of similar or dissimilar alloys. Since alloy production involves intense energy usage via high-temperature heating which subsequently (in most cases) involves the release of greenhouse gases, the effective and efficient usage of industrial alloys and the minimization of pre-mature failures directly reduces the level of greenhouses gases released to the atmosphere.

Financial Impact of Alloy Degradation

Many of the world's physical infrastructure is made of alloys. Alloys are typically solid metallic substances produced by mixing chemical elements (called alloying elements) into a molten or a liquid metallic-based matrix before its solidification via cooling. In many cases, the alloying elements are employed to modify the properties of the metallic-base matrix. For example, an author (Choudary, 2003, p. 228) explained that "the term 'alloy steel' is used to describe those steels to which one or more alloying elements, in addition to carbon, have been deliberately added in order to modify the properties of steel". Alloys, which constitute the material of construction for a significant portion of the global industrial and manufacturing structures and assets employed in the production of goods and services, are expensive when compared with many other types of industrial construction materials such as wood, fiber glass, polymers, composites, etc. Globally, billions of dollars per year are expensed in alloys and asset research, design, manufacture, procurement, fabrication, installation, and operations in applications which include infrastructural, military, industrial, machinery, aeronautical, automobile, residential, transportation, and astronomy. Unfortunately, these very expensive alloy-based assets, equipment, and components are constantly and relentlessly degraded by natural and man-made forces. With the passage of time (in some cases, a few short years), the alloys or assets lose their functions, degrade, and crumble into a useless pile of metallic junk. Unless these unrelenting degradation processes are actively combated, the huge funds expended in creating these assets will be and are wasted. Degraded infrastructure endangers personal safety, increases the cost of production of goods and services and production losses, maintenance cost-overruns, and cost of insurance coverage. Degradation of metallic industrial assets, equipment, and components, costs governments, industries, and citizens billions of dollars a year.

Unfortunately, most of the billions of dollars a year expended on the degradation of metallic components used in industrial assets and equipment are focused on mitigation strategies such as inspection, treatment, and repair – after the degradation is prone to occur or has already occurred.

> *Corrosion causes many problems for humankind. It damages equipment, structures, and the environment in the vicinity of corroded structures. Its cost ranges between 3.1 to 4.5% of the Gross Domestic Product (GDP) in industrialized nations. The annual cost of corrosion in the United States is approximately $300 billion dollars. Canada spends 3.1% of her Gross Domestic Product (GDP), or CAN$32.8 billon, on corrosion prevention and control. This amount, which quantifies only the direct cost of corrosion prevention and control, amounts to approximately two-thirds of the Canadian government annual expenditure on health and education, twice the amount spent on research and development, and thrice the expenditure on national defense. It is estimated that 25% to 30% of annual cost of corrosion could be saved with optimum corrosion management strategies (Obi, 2008, p. 1).*

A lot of study, research, and industrial innovations have significantly improved corrosion preventive measures such as coatings (Jones, 1996, pp. 447-520) (Bahadori, 2015) (Winkelaar, 2009) (Revie & Uhlig, 2008, pp. 269-301) (Schweitzer, 2006), cathodic protection (Jones, 1996, pp. 439-472) (Revie & Uhlig, 2008, pp. 251-267) (Cicek, 2013), and anodic protection (Edeleanu, 1960) (Cicek, 2013, p. 123). Coating prevents degradation by presenting typically non-reactive or inert barrier between the environment and the alloy. Typical materials used for coatings include nitrocellulose, alkyds, acrylics, polyurethanes, and epoxies (Winkelaar, 2009). Cathodic protection involves suppressing corrosion reactions on an alloy by supplying the alloy with electrons from an external source. Cicek (Cicek, 2013) added that "cathodic protection simply involves supplying, from an external source, electrons to the metal to be protected, making it a cathode". For alloys that generate insoluble oxide films in their exposure medium, anodic protection (Cicek, 2013, p. 123) involves facilitating the production and maintenance of the insoluble films on the alloy which thereafter accords the alloy protection in the medium. Scenarios occur where anodic protection is the most practical or economical options to minimize alloy degradation via corrosion. “In chemical plant it is often not economic to use noble metals, and if the solutions are highly oxidizing the other methods are inapplicable. [In these scenarios, anodic protection] is achieved by: (1) Using a metal having an oxide (or other similar corrosion product) which is virtually insoluble in the medium (2) ensuring that sufficient oxidizing agent is always present for the oxide to be formed [and] (3) applying anodic polarization to maintain the oxide in the constant repair” (Edeleanu, 1960). However, one of the most effective methods to minimize the safety risks, economic wastage, and environmental contamination generated by alloy degradation is to select the proper alloys that can perform adequately within the specified exposure environment and to estimate as accurately as possible the lifespan of the alloys – beyond which they need to be replaced. In this way, premature failures (with all the attendant risks and consequences) are significantly minimized. “Often, the most effective method of corrosion prevention is proper selection of materials resistant to the specific corrosive environment (Jones, 1996)”.

It has been estimated that between 3.5% and 5% of an industrialized nation’s income or its Gross National Product (GNP) is spent on corrosion prevention and maintenance or replacement of products lost or contaminated as a result of corrosion reactions, e.g, rusting of the automotive body panels, radiator, and exhaust components. The British Hoar committee prepared a corrosion cost report indicating that corrosion costs 3% of British Gross National Product (GNP), of which 23% can be prevented. Batelle Columbus Laboratories estimated the losses due to corrosion in U.S. equaling 4.9%, while National Bureau of Standards (NIST), found it as 4.2% and both with an error margin of ±30%. Both studies revealed that a maximum of 45%, a minimum of 10%, and an average of 15% of the corrosion cost can be prevented …. The cost of corrosion in the U.S. was considered to be about 3.5 to 4.5% of the country’s gross national product, resulting in about 70 billion dollars of loss in 1976, which increased to 126 billion dollars in 1991. The percentage losses are considered to be even higher in underdeveloped or developing countries, where corrosion protection measures are not sufficiently implemented. However, in practice, it is generally accepted that only up to 30% of the corrosion loss can be prevented (Cicek, 2013, pp. 127-128)

AssessLIFE Software: Simulating Alloy Degradation via the Mechanism of Wet Corrosion

AssessLIFE software aims to select the proper resistant alloy for the defined exposure conditions as well as estimate the lifespan of the alloy during which the alloy provides adequate performance and, thereby, minimizes premature failures. Furthermore, AssessLIFE software addresses the strategic deficiency of employing trailing strategies such as inspections, treatments, and repairs. In addition to enhancing preventive strategies such as coating, cathodic and anodic protection, the AssessLIFE software, in the active battle against industrial asset degradation, focuses on forecasting strategies rather than on mitigation strategies. By employing tested and proven scientific analytical computations, forecasting, prediction, and analytics, the AssessLIFE software plans to significantly reduce the billions of dollars expended via inspection, treatment, and repair of degradation-prone assets and infrastructure.

Figure 1. AssessLIFE software: HomePage

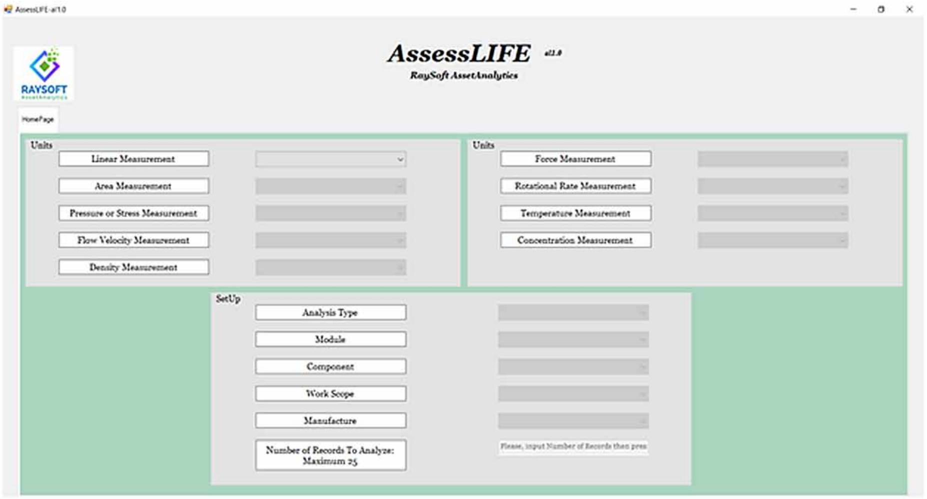


Figure 1 shows the Home Page of the AssessLIFE software. Engineering units constitute the first set of entries into the software. In a sequence, the user is guided to enter all the relevant engineering units needed by the software. The "Setup" box, which is below the "Units" box, contains all the selection boxes where the user configures the software for analysis. The configuration boxes in the "Setup" domain guides the user to define all the major specific details which influence degradation and enables the AssesLIFE software select the appropriate as well as specific computational methods with which to process user input data. The user enters both the asset identifier data and the field data downstream of the HomePage. The configuration boxes in the "Setup" domain include: "Analysis Type"; "Module"; "Components"; "Work Scope"; and "Manufacture". The entry box "Number of

Records To Analyze: Maximum 25" completes the software high-level configuration. The user enters an integer that defines the number of records of assets that will be analyzed. Each entry of the high-level selection boxes helps define a specific use scenario that the software will simulate and analyze. Furthermore, the options selected for each of these high-level configuration boxes progressively defines the downstream user interface pages and the control boxes on these pages that are presented to the user for data entry.

Figure 2 shows the dropdown list for the "Analysis Type" options of the AssessLIFE software. The options include "Wet Corrosion", "Atmospheric Corrosion", "Corrosion Under Insulation", "Erosion", "Wet Corrosion + Erosion", "Metal Fatigue (via rotating element)", and "Corrosion Fatigue (via rotating element)". The options within the "Analysis Type" configuration box define the major degradation mechanisms that drive the failure of industrial assets or alloys. "Corrosion is the degradation of a material by electrochemical or chemical reaction with its environment (Obi, 2008)". Wet corrosion occurs when the mobile ions (or atoms or groups of atoms with a resultant charge) from electrochemical or chemical reactions move within a liquid medium and interface with electrons confined to the metallic structure of the alloy(s). The electrons and ions interact at the interface of the alloy to exchange energy.

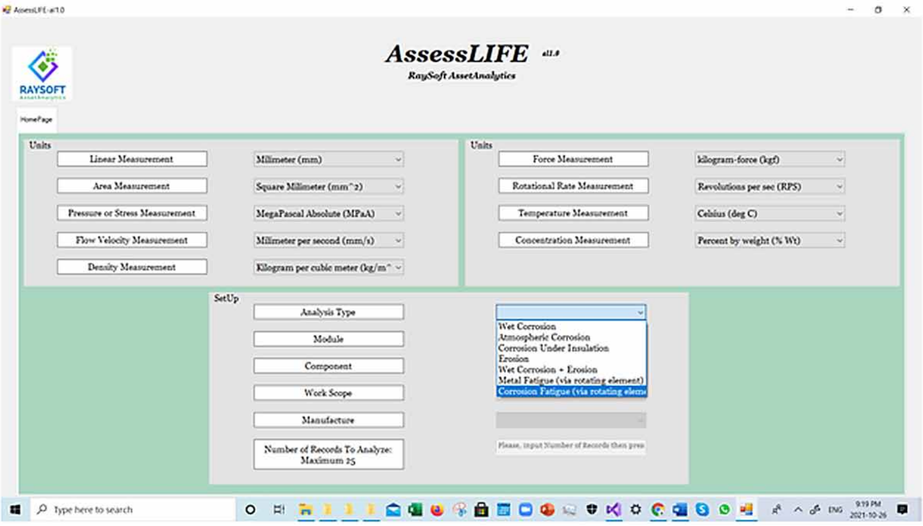
Alloy Degradation: A Multi-Discipline Concept

Corrosion is a multi-dimensional concept that requires a multi-discipline approach to fully appreciate, model, simulate, and integrate into a framework that can estimate the degradation rates of the various corrosion sub-mechanisms as well as forecast the lifespan of assets and alloys subject primarily to the corrosion degradation processes. Corrosion can be viewed from a multidimensional and multidiscipline perspectives which include, but not limited to: the disciplines of electronic, electrical, chemical, process, metallurgical, welding, and mechanical engineering. The corrosion degradation process overlaps with each of the specified disciplines and engages concepts and principles in these disciplines while attempting to arrive at a full and comprehensive understanding of the processes involved in the corrosion mechanism. Some of the overlap between corrosion and the specified disciplines are presented below. The AssessLIFE software models and integrates these mutual interactions within and between these specified disciplines and automates them to compute alloy or asset lifespans and analytics on degradation drivers.

Alloy Degradation in the Electrical and Electronics Engineering Domain

Corrosion engineering, just like electronic engineering, discusses the movement of electrons within an alloy or structure. The electrons naturally move from areas of high electron density to areas of lower electron density. However, unlike in electronic engineering where the electron flow is controlled to perform useful work, the resultant energy from corrosion processes is largely wasted. "Electronics is the field of science that uses electrical principles to perform other useful work … Electricity is moving electrons. An electron is a tiny particle that is inside the atoms that make up everything we can feel, see, and even not see. If we can get some electrons moving together in a wire, electrical or electronic component, we can control them to do many useful things, such as amplification (Frenzel Jr., 2018, pp. 6-7). When more electrons accumulate in a region of the alloy or structure thereby increasing the electron density of the region, this region of higher electronic density generates a potential difference between other adjacent regions with lower electronic density. It is this potential difference or voltage that drives electron movement. In corrosion engineering, this electron movement driven by a voltage causes metal loss; while in electrical and electronic engineering, this voltage driven electron movement is principally harnessed to perform work. "Voltage is defined as an electromotive force that moves or pushes electrically charged particles like electrons, holes, negatively charged ions or positively charged ions. … Current consists of movement of electrons, ions, or simply charged particles (Rauf, 2014, pp. 1-2). Blume (Blume, 2007, p. 5) added that "Voltage is the electric power system's potential energy source. Voltage does nothing by itself but has the potential to do work. Voltage is a push or a force. Voltage always appears between two points. Voltage always tries to push or pull current. Therefore, when a complete circuit or closed-loop path is provided, voltage will cause current to flow. The resistance in the circuit will reduce the amount of current flow and will cause heat to be provided". Hence, the corrosion process which includes metal loss from electron movement driven by voltage, overlaps the fields of electronic and electrical engineering where voltage drives current which is typically harnessed to perform useful work.

Figure 2. AssessLIFE "analysis type" options



Units

Linear Measurement: Millimeter (mm)
Area Measurement: Square Millimeter (mm^2)
Pressure or Stress Measurement: MegaPascal Absolute (MPaA)
Flow Velocity Measurement: Millimeter per second (mm/s)
Density Measurement: Kilogram per cubic meter (kg/m^

Units

Force Measurement: kilogram-force (kgf)
Rotational Rate Measurement: Revolutions per sec (RPS)
Temperature Measurement: Celsius (deg C)
Concentration Measurement: Percent by weight (% Wt)

SetUp

Analysis Type
Module
Component
Work Scope
Manufacture
Number of Records To Analyze: Maximum 25
Wet Corrosion
Atmospheric Corrosion
Corrosion Under Insulation
Erosion
Wet Corrosion + Erosion
Metal Fatigue (via rotating element)
Corrosion Fatigue (via rotating eleme
Please, input Number of Records then pres
Type here to search
ENG
9:19 PM
2021-10-26

Alloy Degradation in the Chemical Engineering Domain

Corrosion processes overlap with the field of chemical engineering. Corrosion processes always involve chemical reactions or the exchange of chemical ions. While different electron densities form in different regions of the alloy and electrons translate in the alloy or structure, simultaneously, chemical ions migrate about in the liquid or aqueous medium. During the corrosion processes, metal atoms at the anode electrode lose their electrons – become charged particle or ions – and enter into liquid or aqueous phase. The motions of chemical ions are identical to electron flow processes in electrical and electronic engineering. Metal atoms enter into solution in a process called oxidation reactions – which occurs at the anode electrodes. At the interface between the cathode and liquid, these liberated electrons reduce chemical species or ions in solution during reactions called reduction reactions. Hence, oxidation reactions occur at the anode electrode while reduction reactions occur at the cathode electrode. From the corrosion perspective, the oxidation and reduction reactions are one of the distinguishing frontiers between how corrosion processes overlap with electrical and electronic engineering and how the corrosion processes overlap with chemical engineering. Hence, unlike in the electrical and electronic domains, the chemical domain involves the oxidation and reduction of chemical species in solution. Chemical reactions can be classified under two separate but interrelated regimes, namely: the drive for the reaction to occur – called thermodynamics, and the rate of chemical reaction - covered by chemical kinetics. On the one hand, chemical thermodynamics can be considered analogous to voltage-influences in electrical and electronic domains where the voltage is the driver for current to flow between regions of different voltage levels. "Chemical … thermodynamics help us understand how much energy is released or consumed during a reaction, which reactions are favored, and how to enhance a reaction system to produce the most desired products and minimize raw materials and energy consumption" (Hipple, 2017, pp. 45-67). For corrosion reactions specifically, Marcel Pourbaix (Pourbaix, 1974) established pH versus potential (in volts) maps of thermodynamic equilibrium diagrams called Pourbaix diagrams. The Pourbaix diagram indicates the various regions in an alloy-water system where the system experiences the drive to corrode, remain passive, or become immuned (or inert) (Cicek, 2013, pp. 75-96). Figure 3 shows an illustration of Pourbaix thermodynamic corrosion diagram for aluminum. On the other hand, chemical kinetics is concerned with the rate or speed of chemical reactions – and it is analogous to electron flow domains in electrical and electronic engineering. Since corrosion reactions are chemical reactions, these corrosion reactions operate under the principles of chemical kinetics. Chemical kinetics describes how fast a reaction reaches its end-point or equilibrium (Hipple, 2017, pp. 55-67). Figure 4 shows a representation of the corrosion kinetics diagram of pure aluminum.

Alloy Degradation in the Process Engineering Domain

Corrosion processes also interface with process engineering. Corrosion can be described as the flow of electrons in an alloy or structure resulting in metal loss as the alloy or structure interacts with its exposure environment. Hence, the variables of the exposure environment also influence corrosion processes. In industrial settings, influential environmental variables that drive corrosion are the typical process variables of Plant operations. "A process is any operation or series of operations that causes physical or chemical changes in a substance or a mixture of substances" (Ghasem & Henda, 2009, pp. 11-32). The process variables include temperature, pressure,

concentration, flow rates, pH, etc. Gladstone describes "the process variable [as] set of quantities that defines the operating conditions of a [chemical] system …" (Glastone & Mehra, 2011, p. 37). Hippe (Hipple, 2017, p. 50) reinforced that process variables affect the outcome of chemical reactions when he stated that the point of attainment of equilibrium of a chemical reaction system "will be affected by temperature as well as the ratios of reactants, and for gases, the pressure as well." Sedriks (Sedriks, 1996) discussed the different process variables that affect corrosion reactions specifically.

Figure 3. Illustration of Pourbaix diagram for aluminum
(Obi, 2008, p. 12)

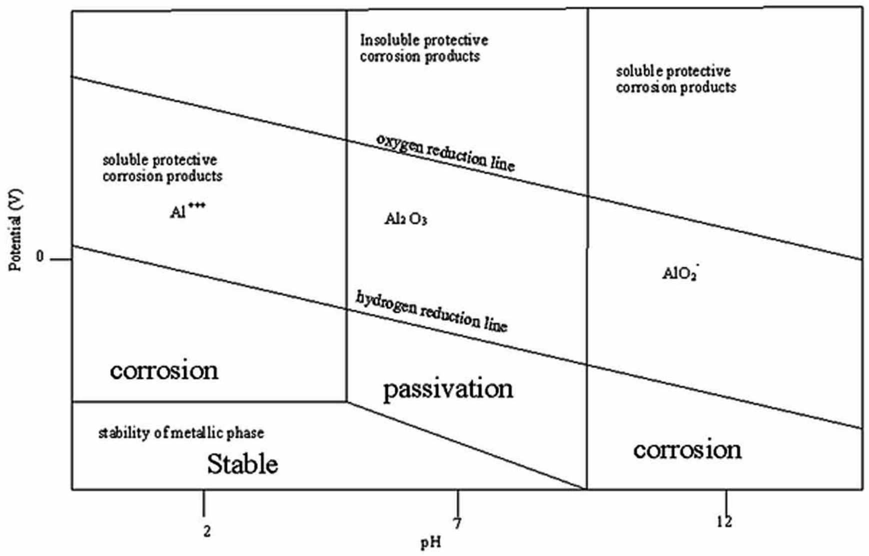
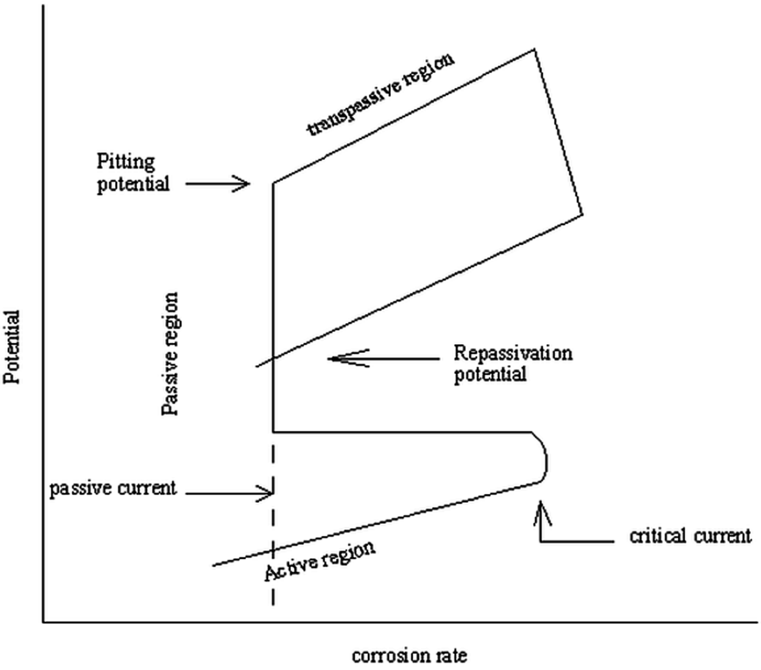

Insoluble protective corrosion products
soluble protective corrosion products
oxygen reduction line
soluble protective corrosion products
Al+++
Al2 O3
AlO2-
Potential (V)
0
hydrogen reduction line
corrosion
passivation
stability of metallic phase
Stable
corrosion
2
7
12
pH

Figure 4. Representation of the Corrosion kinetics behavior of pure aluminum
(Obi, 2008, p. 14)



Alloy Degradation in the Mechanical Engineering Domain

The corrosion processes are mutually influenced by the decision made and actions taken in the mechanical, metallurgical, and welding domains. Mechanical, metallurgical, and welding engineering also overlap with corrosion engineering. Mechanical engineering utilizes the principles of energy, motion, and force to understand and manipulate systems. Energy, which is the capacity to do work, as well as motion and force, influence atomic and electronic behavior in an alloy or structure. Increased energy, motion, and force may cause the atoms of an alloy or structure to aggregate or to increase its electron density in certain regions or to vibrate more. The new states of the electrons may facilitate corrosion – if the electrons translate within alloy or structure. Mechanical stress and deformation can significantly influence corrosion processes (Haanappel & Stroosnijder, 2001).

Alloy Degradation in the Metallurgical Engineering Domain

In Metallurgical engineering, it is shown that atoms and molecules (which are the building blocks of alloys and structures) arrange themselves in a patten which can be termed the crystal structure (Choudary, 2003). The entities that constitute the crystal structure interact via processes such as atomic, metallic, ionic, covalent bonding as well as via Van Der Waals forces (Choudary, 2003). Groups of these atomic and molecular entities can aggregate to form grains whose boundaries are called grain boundaries (Choudary, 2003). "Grain boundaries consist of atoms in non-equilibrium positions, and as such they are high-energy regions of stability " (Choudary, 2003). The structure and compositions of grains and, particularly, grain boundaries influence both the drive for corrosion to occur (corrosion thermodynamics) and the rate of corrosion processes (corrosion kinetics). In many cases, the highly-alloyed, high energy, and high electron density grain boundary corrode preferentially to the grain interior (which in comparison to the grain boundary composition, has fewer alloying elements, lower energy, and lower electron density). The difference in electron density between the grain boundary and grain (interior) can drive electrons from the boundary to the interior resulting in the corrosion of the boundaries. This process typically results in intergranular corrosion. Figure 5 shows the grains and grain boundaries of Mg_2Si phase in aluminum alloy A535 matrix before exposure to a corroding medium of NaCl solution. Figure 6 shows the corroded Mg_2Si phase in the aluminum A535 matrix after 14 days of exposure in a neutral NaCl solution. The Mg_2Si phase had higher electron activity and density compared to the aluminum A535 matrix and thereby lost electrons to the matrix and, consequently, corroded. Figure 7 shows a higher magnification image of the corrosion damage of the aluminum A535 sample. It can be seen that at high magnification that corrosion damage preferentially selects certain locations on the surface of the sample. Typically, high-energy, high-electron density, and high-activity locations selectively undergo metal loss during corrosion activity.

Alloy Degradation in the Welding Engineering Domain

Welding engineering describes the localized heating and rapid cooling of alloys to achieve a metallic joint (Phillips, 2016) (Singh, 2012) (Lippold, Welding Metallurgy and Weldability, 2015) (Kotecki & Lippold, 2005) (Dupont, Lippold, & Kiser, 2009). The effects of welding includes; redistribution of alloying elements, addition of alloying elements via the filler-metal, creation of new grains and grain boundaries, and acceleration of grain growth in the different regions of the weld (or weldment) (Dupont, Lippold, & Kiser, 2009) (Lippold, 2015) (Ghosh, 2016). As seen with the grain dynamics in metallurgical engineering, redistribution, creation, addition, and growth acceleration of grains and grain boundaries influence the possibility of corrosion and rates of corrosion reactions. Furthermore, welding can generate residual stresses which can induce both mechanical fractures and corrosion degradation. The different regions of a weld can have different chemical compositions, alloying elements distribution, sizes of grains, compositions of grain boundaries, and different electron densities. All these factors can induce corrosion degradation of the weldment (The Materials Information Society, 2006).

AssessLIFE Software: Simulating Alloy Degradation via the Mechanism of Atmospheric Corrosion

Besides “Wet Corrosion”, Figure 2 also shows that the AssessLIFE software has “Atmospheric Corrosion” and “Corrosion Under Insulation” packages with which to analyze and estimate lifespans of alloys and assets under the degradation mechanisms of atmospheric corrosion and

corrosion under insulation. Atmospheric corrosion is corrosion degradation that occurs under atmospheric conditions. Similar to wet corrosion, atmospheric corrosion involves corrosion thermodynamics and kinetics reaction processes. However, unlike wet corrosion which is driven by process variables (such as industrial stream temperature, pressures, concentrations, and pH), atmospheric corrosion is driven by process variables under atmospheric conditions (such as atmospheric pressure, temperature, dewpoint, time of wetness, as well as solids, liquids, and gaseous atmospheric contaminants) (Schweitzer, 2006, pp. 39-66). Atmospheric corrosion is also location dependent. Different locations contain different degrees of atmospheric variables which influence the corrosion processes and result in different degrees of severity of corrosion damage.

Figure 5. A micrograph showing Mg_2Si grains in A535 matrix and surrounding grain boundaries before immersion in salt solution
(Obi, 2008, p. 63)

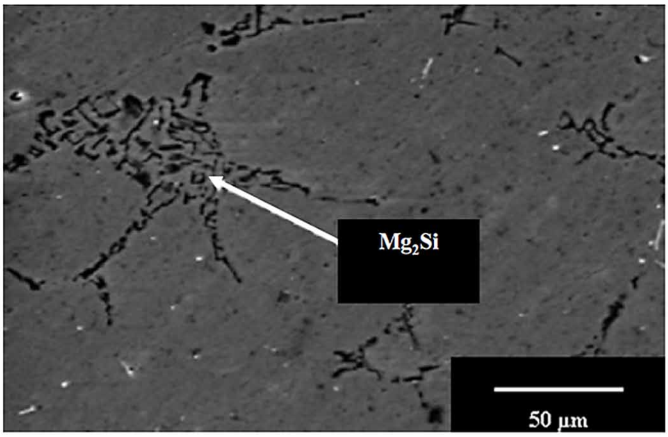


Figure 6. Optical micrograph showing the corroded surface of A535 specimen immersed in neutral salt solution for 14 days
(Obi, 2008, p. 65)

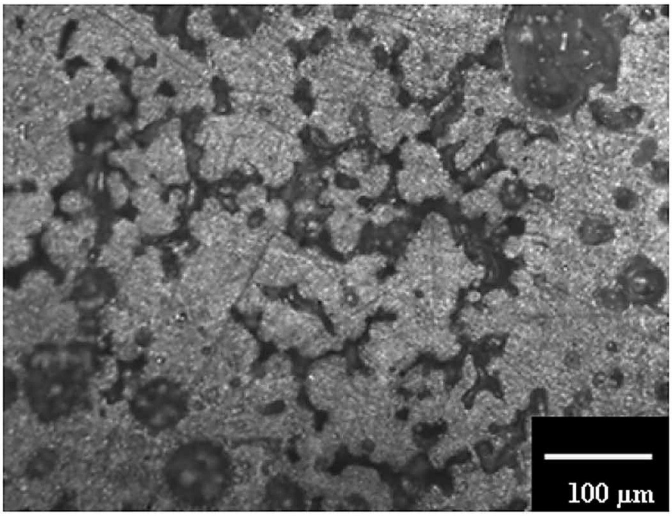
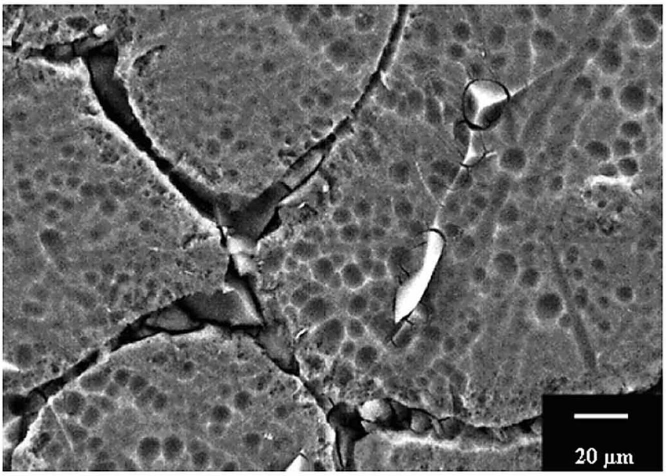


Figure 7. A micrograph of A535 alloy in neutral 3.5wt% NaCl solution for 14 days (Obi, 2008, p. 65)



> *Because [atmospheric] corrosion rates are affected by local conditions, atmospheres are generally divided into the following major categories: Rural, Industrial, and Marine. … For all practical purposes, the more rural the area, with little or no heavy manufacturing operations, or with very dry climatic conditions, the less will be the problem of atmospheric corrosion. … Marine environments are subject to chloride attach resulting from the deposition of fine droplets of crystals formed by evaporation of spray that has been carried by the wind from the sea (Schweitzer, 2006, pp. 40-41).*

AssessLIFE Software: Simulating Alloy Degradation via the Mechanism of Corrosion Under Insulation

Corrosion under insulation is corrosion degradation that occurs below insulation applied typically on the atmosphere-facing-side of assets to prevent the ingress of moisture and other air-borne contaminants which can drive corrosion attack of the asset. Moisture ingress via the insulation to the asset-insulation interface is a major challenge with preventing corrosion under insulation damage (Zelinka, Glass, & Derome, 2014). At dew point temperature on exposure surfaces, liquid water condenses from water vapor in the air and wets the exposed surfaces. “The dew point is the temperature a parcel of air needs to be cooled at constant pressure for saturation (100% relative humidity) to occur.” (Bui, Johnson, & Wasko, 2019). Similarly, some researchers (Ukhurebor, Batubo, Abiodun, & Enoyoze, 2017) defined the dew point temperature as “the temperature at which the moisture/liquid water (water vapor) in the air begins to condense …". The implication of dew point temperature for corrosion under insulation becomes clear when one considers that when assets operating with high temperature streams or fluids are shut down for maintenance or production changes, the asset cools down. However, as the asset cools, it traverses the dew point temperature of the surrounding air on its surfaces. At and below the dew point temperature of the surrounding air, at the asset-insulation interface, water vapor within the pores of the insulation can condense and provide an environment for corrosion under insulation attack on the asset. Different types of insulation can provide different degrees of resistance to condensed water accumulation at the asset-insulation interface, and therefore, provide varying degrees of protection to the corrosion under insulation attack.

AssessLIFE Software: Simulating Alloy Degradation via the Mechanism of Erosion

Figure 2 also shows that the AssesLIFE software possesses "Erosion" and "Wet Corrosion + Erosion" packages. Unlike corrosion which involves chemical reactions, erosion is the physical removal of tiny bits of the alloy by either the fluid or stream itself (fluid- or stream- induced erosion) or by the stream-borne particles (solid-particle erosion). Fluid flow is governed by two distinct regimes: the laminar-flow region and the turbulent-flow region (Taghavi-Zenouz, Salari, & Etemadi, 2008). "When the flow is orderly and predictable, the flow pattern is often amenable to mathematical solutions. These flows are called laminar. In laminar flow, the individual fluid particles move along their trajectories independent of the particles in the adjacent layers" (Elsevier, 1991). The research (Elsevier, 1991) also adds "[t]he beautiful laminar flows … exist only under special conditions. If the flow conditions are altered due to increased velocity or temperature, a new flow picture may result. The mathematical solutions to the equations must also change accordingly. When there are observed waves and vortices in a flow field, the equations must yield solutions that contain these phenomena. The process of change from laminar to wavy or turbulent flow can be developed in the basic flow equations and is known as instability analysis or instability theory." In summary, turbulent flow is characterized by wakes, eddies, energy and momentum transitions and losses, unpredictable fluid property changes, and a "rough" flow behavior. It is typically this "rough exchange" that detaches tiny bits of the alloy. Research (Shehadeh, Anany, Saqr, & Hassan, 2014) (Badr, Habib, Ben-Mansour, & Said, 2005) has shown that turbulent flow (which initiates at a certain laminar-to-turbulent transition flow velocity) does increase significantly the erosion damage on alloys or assets. Shehadeh et al (Shehadeh, Anany, Saqr, & Hassan, 2014) found that "[within] the chosen flow rates and contamination levels, … the rates of erosion increase linearly with the increase of flow velocities …. Generally speaking, the erosion rate was doubled on the transition from the laminar to the turbulent flow regime ….” The works of Badr et al (Badr, Habib, Ben-Mansour, & Said, 2005) revealed that “the results showed [a] strong dependence of erosion on both particle size and flow velocity … “. In addition to flow velocity, stream density also contributes to erosion damage. Stream density represents the weight (or force) of the fluid flung on to the alloy surface driven by flow velocity. Fluids with greater density are heavier than lighter fluids and tend to remove greater numbers of tiny bits of the alloy surface and, thereby, inflict more severe erosion. “Density is the sum of the mass of the molecules in a designated volume, that is, mass per unit volume. Kinetic energy is half the average molecular mass times velocity squared in this volume” (Elsevier, 1991, p. 50). The kinetic and momentum (that is, mass of fluid particles multiplied by the particle velocity) of fluid particles are thereby influenced by the fluid density. “Each molecule [within the liquid] carries momentum with it in its random migration” (Elsevier, 1991, p. 60). Both fluid kinetic energy and momentum influence energy transfer to the alloy surface and affect the severity of erosion damage inflicted on the alloy.

Erosion by stream-borne particles or solid-particle erosion occurs when solid-particles rather than the fluid itself is the principal agent of the erosion damage. A fluid or stream laden with solid particles moving at a high fluid velocity relative to the boundary of its container will impinge on the container boundary or scour the boundary of the container thereby eroding it.

> *Small solid particle impact erosion of materials occurs by the removal of material from a surface by a micromechanical deformation/fracture process. On ductile materials, the impacting particles cause severe, localized plastic strain to occur that eventually exceeds the strain to failure of the deformed material. On brittle materials, the force of the erodent particles causes cracking and chipping off of micro-size pieces. These two relatively simple mechanisms are the essence of small solid particle erosion (Levy, Solid Particle Erosion and Erosion-Corrosion of Materials, 1995, p. 1).*

Parameters which influence erosion damage via solid-particle erosion include: erodent density, size, hardness, shape and impingent angle as well as target material hardness and density. “Erosion-material wastage is dependent on many interrelated factors that include the properties and structures of the target materials, the macroexposure and microexposure conditions, and the physical and chemical characteristics of the erodent particles” (Levy, Solid Particle Erosion and Erosion-Corrosion of Materials, 1995, p. 1). AssessLIFE software has the capability to assess the contribution of the various factors which influence both fluid-induced erosion and solid-particle erosion.

AssessLIFE Software: Simulating Alloy Degradation via the Mechanism of Erosion Corrosion

In addition to erosion, Figure 2 shows that the AssessLIFE software offers the "Erosion + Wet Corrosion" package for alloy degradation analysis. "Erosion + Wet Corrosion" is typically termed erosion corrosion. Erosion corrosion is the synergistic degradation resulting from the combination of wet corrosion and erosion degradation processes. "The term erosion corrosion is a combined action of mechanical abrasion and wear on the surface of metal as a consequence of fluid motion and corrosion." (Cicek, 2013, p. 54). Erosion action removes the passive films on some alloys or the boundary surface of other alloys, and consequently exposing the inner vulnerable surface to the chemical reactions of corrosion attack. This iterative process repeats and the alloy is in a worse condition than if it was only under attack by either corrosion or erosion mechanism alone.

AssessLIFE Software: Simulating Alloy Degradation via the Mechanism of Metal Fatigue

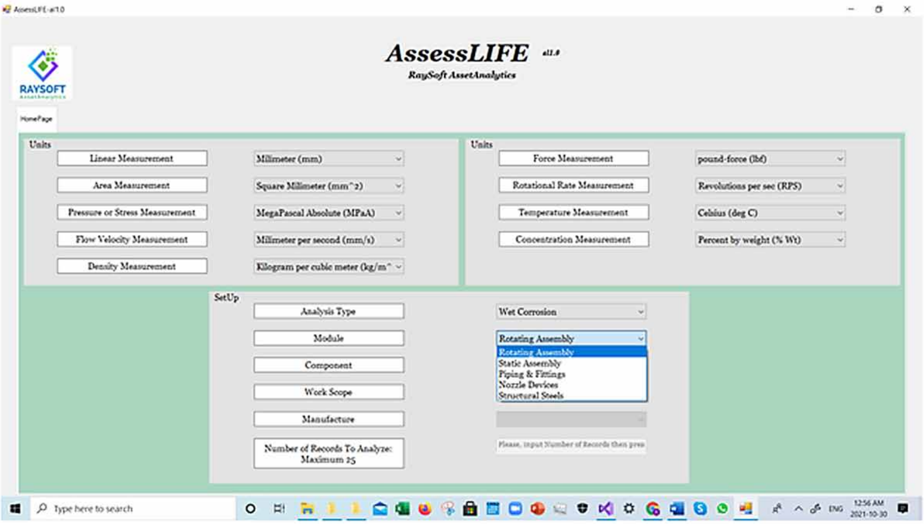
Figure 2 shows that "metal fatigue (via rotating element)" and "corrosion fatigue (via rotating element)" are the last analysis packages in the current version of the AssessLIFE software. Metal fatigue is a degradation mechanism which occurs when an alloy is bent back-and-forth until cracks initiate after a defined number of cycles and propagate until the alloy fractures. Back-and-forth motions represent alternating, cyclic, fluctuating, or vacillating loadings. Back-and-forth motions are typically impacted to an alloy, component, device, or structure by alternating, vacillating, fluctuating, and cyclic forces and stresses. "Fatigue is the progressive, localized, permanent structural change that occurs in materials subjected to fluctuating stresses and strains that may result in cracks or fracture after a sufficient number of fluctuations" (Edited by Boyer Howard E., 2020, Ninth Printing, p. 1). Fatigue failure is a progressive failure driven by cyclic stress application. It is a fracture failure that occurs over time. It contrasts with the sudden stress overload failure that can occur when inadequate cross-section is implemented on a load-carrying structural member or machine element. Similar to corrosion and erosion failures, metal fatigue is a time-dependent failure mechanism.

Mechanical failure modes can be grouped into two categories: (1) instant, force, or moment dependent [or time independent], (2) time dependent. Bending, shear, torsion, and buckling happen instantly if the force/moment applied to the part is more than the design criteria. It is quite easy to calculate these failure modes, since there is no uncertainty. On the other hand, erosion, corrosion, fatigue, creep, and *thermal shock are time and environment dependent and cannot be controlled easily throughout the life of the part, and moreover more than one can occur at the same time causing the life of a part to decrease exponentially (Kececi, 2019).*

AssessLIFE Software: Simulating Alloy Degradation via the Mechanism of Corrosion Fatigue

While metal fatigue occurs in the absence of a degrading environment or corrosive solution, corrosion fatigue is fatigue process exposed to a corrosive medium. The synergy of corrosion and fatigue which occurs during corrosion fatigue causes failure to occur at a short number of cycles – than with plane metal fatigue failure. With both metal fatigue and corrosion fatigue, “the process of [failure] consists of three stages: (1) Initial fatigue damage leading to crack nucleation and crack initiation, (2) progressive cyclic growth of a crack(crack propagation) until the remaining uncracked cross section of a part becomes too weak to sustain the loads imposed, (3) final, sudden fracture of the remaining cross section” (Edited by Boyer Howard E., 2020, Ninth Printing, p. 1).

Figure 8. AssessLIFE “module” options



Units

Linear Measurement: Millimeter (mm)
Area Measurement: Square Millimeter (mm^2)
Pressure or Stress Measurement: MegaPascal Absolute (MPaA)
Flow Velocity Measurement: Millimeter per second (mm/s)
Density Measurement: Kilogram per cubic meter (kg/m^

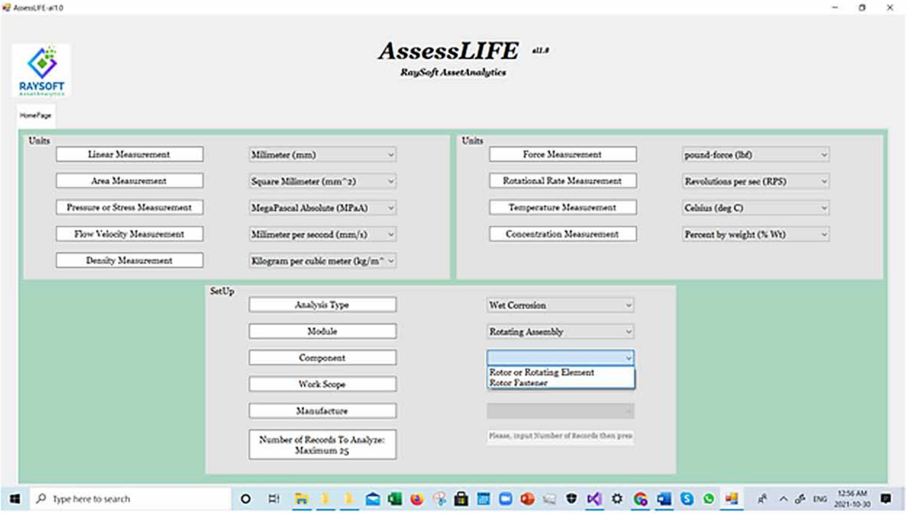
Units

Force Measurement: pound-force (lbf)
Rotational Rate Measurement: Revolutions per sec (RPS)
Temperature Measurement: Celsius (deg C)
Concentration Measurement: Percent by weight (% Wt)

SetUp

Analysis Type: Wet Corrosion
Module: Rotating Assembly
Component
Work Scope
Manufacture
Number of Records To Analyze: Maximum 25: Please, input Number of Records then pres

Figure 9. AssessLIFE "component" options when "module" option 'rotating assembly' is selected



Units

Linear Measurement	Millimeter (mm)
Area Measurement	Square Millimeter (mm^2)
Pressure or Stress Measurement	MegaPascal Absolute (MPaA)
Flow Velocity Measurement	Millimeter per second (mm/s)
Density Measurement	Kilogram per cubic meter (kg/m^

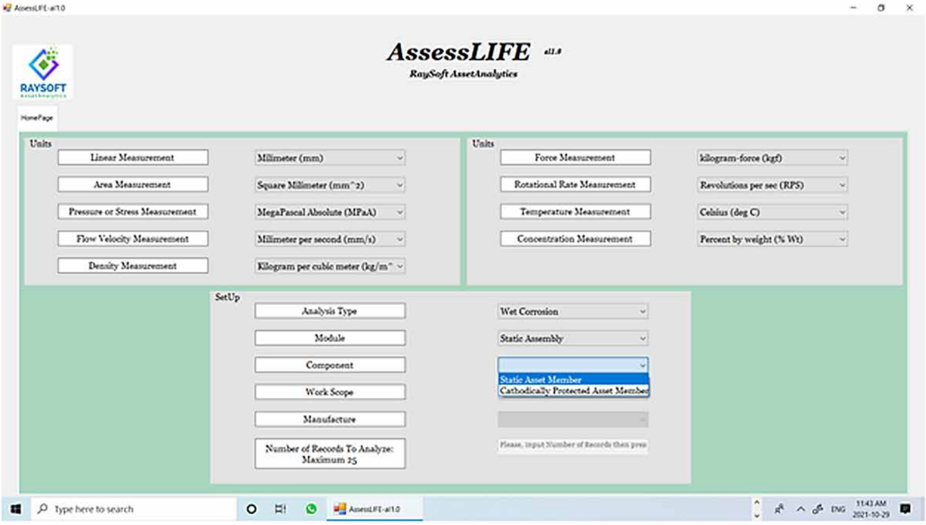
Units

Force Measurement	pound-force (lbf)
Rotational Rate Measurement	Revolutions per sec (RPS)
Temperature Measurement	Celsius (deg C)
Concentration Measurement	Percent by weight (% Wt)

SetUp

Analysis Type	Wet Corrosion
Module	Rotating Assembly
Component	Rotor or Rotating Element Rotor Fastener
Work Scope	
Manufacture	
Number of Records To Analyze: Maximum 25	Please, input Number of Records then pres

Figure 10. AssessLIFE "component" options when "module" option 'static assembly' is selected



Units

Linear Measurement	Millimeter (mm)
Area Measurement	Square Millimeter (mm^2)
Pressure or Stress Measurement	MegaPascal Absolute (MPaA)
Flow Velocity Measurement	Millimeter per second (mm/s)
Density Measurement	Kilogram per cubic meter (kg/m^

Units

Force Measurement	kilogram-force (kgf)
Rotational Rate Measurement	Revolutions per sec (RPS)
Temperature Measurement	Celsius (deg C)
Concentration Measurement	Percent by weight (% Wt)

SetUp

Analysis Type	Wet Corrosion
Module	Static Assembly
Component	Static Asset Member Cathodically Protected Asset Membe
Work Scope	
Manufacture	
Number of Records To Analyze: Maximum 25	Please, input Number of Records then pres

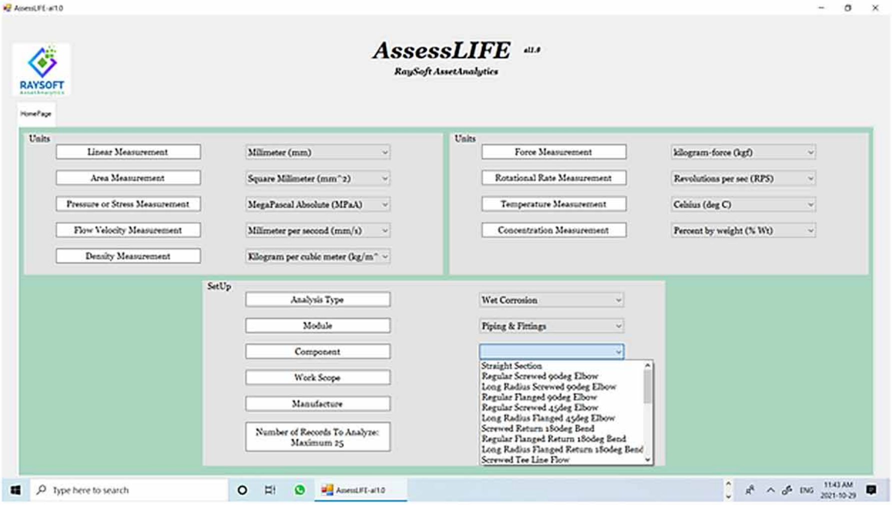
AssessLIFE Software: Configuration Options

The AssessLIFE software presents users with several configuration options which enable the user define the specific details of the users' application scenario with the goal that the software is provided with sufficient information to model, simulate, and analyze the application scenarios. Figure 8 shows the options for the "Module" configuration selection box. The "Module" options present the different assemblies that can be analyzed by the AssessLIFE software. An assembly is a collection of parts or components joined together using various joining or coupling methods. The assemblies include rotating assembly, static assembly, piping and fittings assembly, nozzle assembly, and structural steel assembly. The "Module" configuration box defines the assembly type and feeds into the "Component" configuration selection box options that further defines the type of member of the selected assembly to be analyzed. Figure 9 shows the "Component" configuration selection box options when the "Module" configuration selected option is 'Rotating Assembly'.

When 'Rotating Assembly' is selected in the "Module" box, only 'Rotor or Rotating Element' and 'Rotor Fastener' are available for analysis by the 'Wet Corrosion' degradation process or mechanism. As shown in Figure 10, when 'Static Assembly' is the selected option at the "Module" level, the options at the component level are 'Static Asset Member' or 'Cathodically Protecccted Asset Member'. Similarly, the selection of 'Piping & Fittings' at the "Module" configuration level, generates a list of piping components and fittings at the "Component" level options as Figure 11 shows. In the same vein, in Figure 12, when 'Nozzle Devices' is selected at the "Module" level, a list of nozzle related components is available as options at the "Component" configuration level. Lastly, as shown in Figure 13, selecting 'structural steels' at the module level, displays 'structural member' as the only option available for selection at the "Component" configuration level. Hence, the AssessLIFE software enables users mirror their real-life applications via choosing the most appropriate options in the configuration boxes with the goal that the analysis takes into account the specific details of the user application scenarios.

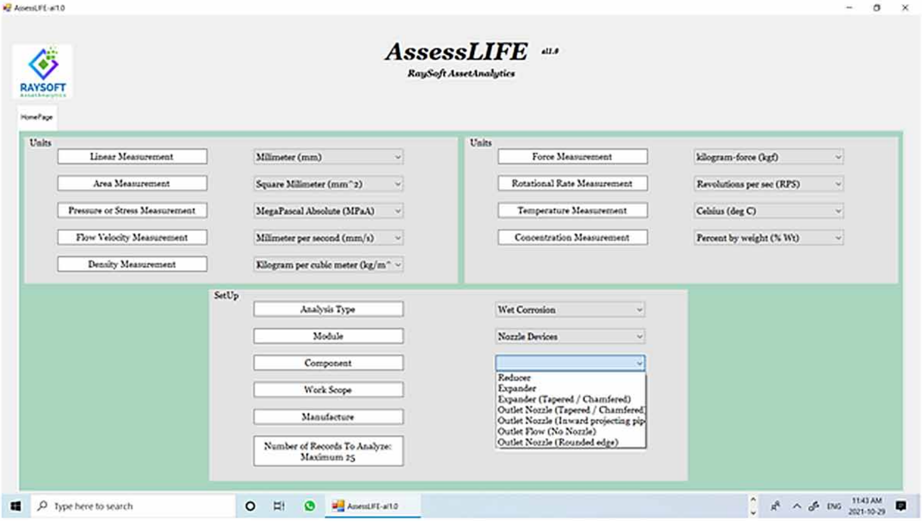
When the "Component" configuration has been decided and selected, the "Work Scope" configuration selection box is enabled for user input. Figure 14 shows the options available to the user in the "Work Scope" selection box: 'Member Envelope or Shell' and 'Sleeve or Patch on Member Envelope'. The term 'Member Envelope or Shell' denotes analysis applied to the original envelope or boundary of the asset member specified, while 'Sleeve or Patch on Member Envelope' denotes analysis applied to a repair sleeve or patch on the member's original boundary or envelope. Figure 15 shows that below the "Work Scope" configuration level in the AssessLIFE software is the "Manufacture" configuration. The "Manufacture" configuration box enables the user specify the method of manufacture of the selected member to be analyzed. The method of manufacture of a part or component can often influence the type or speed of degradation that the member experiences in service. The "Manufacture" dropdown list includes "Welded Without Filler Metal (Autogenous)", "Welded With Filler Metal", "Fastened", and "Cast".

Figure 11. AssessLIFE "component" options when "module" option 'piping and fittings' is selected


AssessLIFE-a1.0
AssessLIFE a1.0
RaySoft AssetAnalytics
RAYSOFT
HomePage
Units
SetUp
Straight Section
Regular Screwed 90deg Elbow
Long Radius Screwed 90deg Elbow
Regular Flanged 90deg Elbow
Regular Screwed 45deg Elbow
Long Radius Flanged 45deg Elbow
Screwed Return 180deg Bend
Regular Flanged Return 180deg Bend
Long Radius Flanged Return 180deg Bend
Screwed Tee Line Flow
Type here to search
11:43 AM
2021-10-29

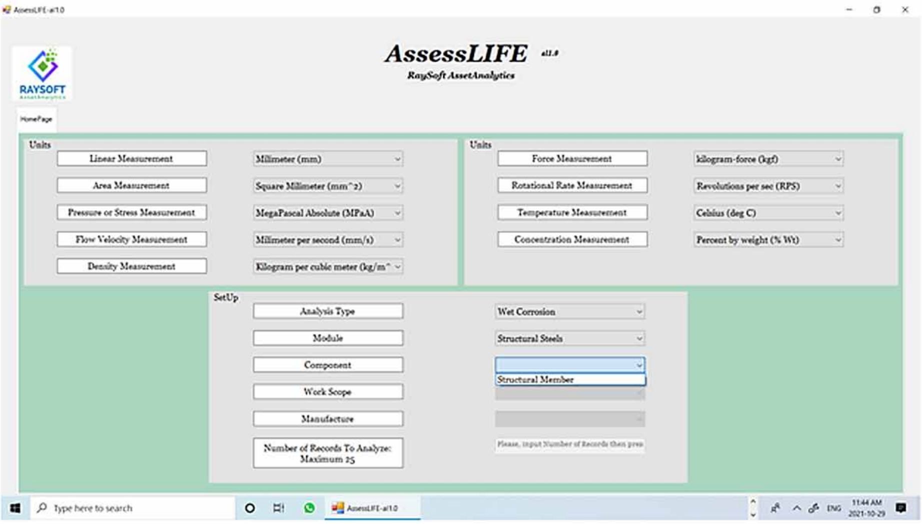
Linear Measurement: Millimeter (mm)
Area Measurement: Square Millimeter (mm^2)
Pressure or Stress Measurement: MegaPascal Absolute (MPaA)
Flow Velocity Measurement: Millimeter per second (mm/s)
Density Measurement: Kilogram per cubic meter (kg/m^
Force Measurement: kilogram-force (kgf)
Rotational Rate Measurement: Revolutions per sec (RPS)
Temperature Measurement: Celsius (deg C)
Concentration Measurement: Percent by weight (% Wt)
Analysis Type: Wet Corrosion
Module: Piping & Fittings
Component:
Work Scope
Manufacture
Number of Records To Analyze: Maximum 25

Figure 12. AssessLIFE "component" options when "module" option 'nozzle devices' is selected



Linear Measurement: Millimeter (mm)
Area Measurement: Square Millimeter (mm^2)
Pressure or Stress Measurement: MegaPascal Absolute (MPaA)
Flow Velocity Measurement: Millimeter per second (mm/s)
Density Measurement: Kilogram per cubic meter (kg/m^
Force Measurement: kilogram-force (kgf)
Rotational Rate Measurement: Revolutions per sec (RPS)
Temperature Measurement: Celsius (deg C)
Concentration Measurement: Percent by weight (% Wt)
Analysis Type: Wet Corrosion
Module: Nozzle Devices
Component:
Work Scope
Manufacture
Number of Records To Analyze: Maximum 25

Figure 13. AssessLIFE "component" options when "module" option 'structural steels' is selected



AssessLIFE-al1.0

AssessLIFE al1.0

RaySoft AssetAnalytics

HomePage

Units

Linear Measurement: Millimeter (mm)

Area Measurement: Square Millimeter (mm^2)

Pressure or Stress Measurement: MegaPascal Absolute (MPaA)

Flow Velocity Measurement: Millimeter per second (mm/s)

Density Measurement: Kilogram per cubic meter (kg/m^

Units

Force Measurement: kilogram-force (kgf)

Rotational Rate Measurement: Revolutions per sec (RPS)

Temperature Measurement: Celsius (deg C)

Concentration Measurement: Percent by weight (% Wt)

SetUp

Analysis Type: Wet Corrosion

Module: Structural Steels

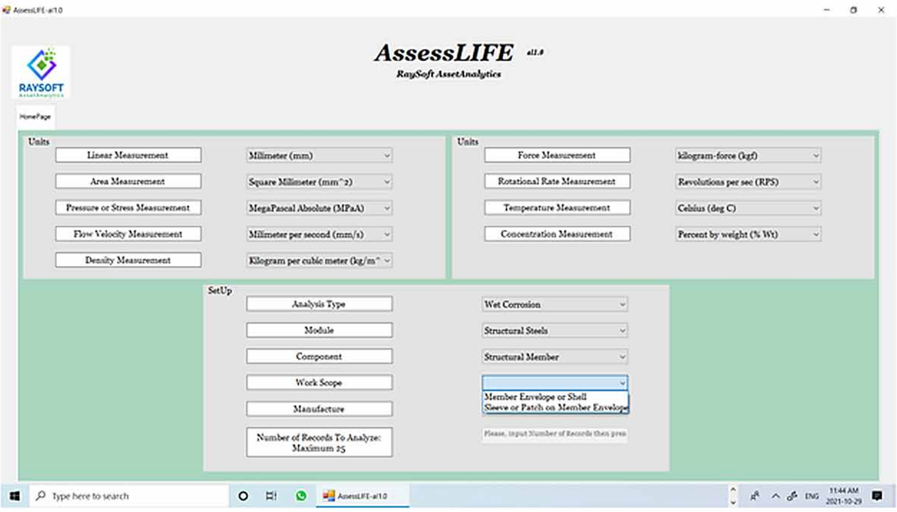
Component: Structural Member

Work Scope

Manufacture

Number of Records To Analyze: Maximum 25: Please, input Number of Records then pres

Figure 14. AssessLIFE "work scope" options



AssessLIFE-al1.0

AssessLIFE al1.0

RaySoft AssetAnalytics

HomePage

Units

Linear Measurement: Millimeter (mm)

Area Measurement: Square Millimeter (mm^2)

Pressure or Stress Measurement: MegaPascal Absolute (MPaA)

Flow Velocity Measurement: Millimeter per second (mm/s)

Density Measurement: Kilogram per cubic meter (kg/m^

Units

Force Measurement: kilogram-force (kgf)

Rotational Rate Measurement: Revolutions per sec (RPS)

Temperature Measurement: Celsius (deg C)

Concentration Measurement: Percent by weight (% Wt)

SetUp

Analysis Type: Wet Corrosion

Module: Structural Steels

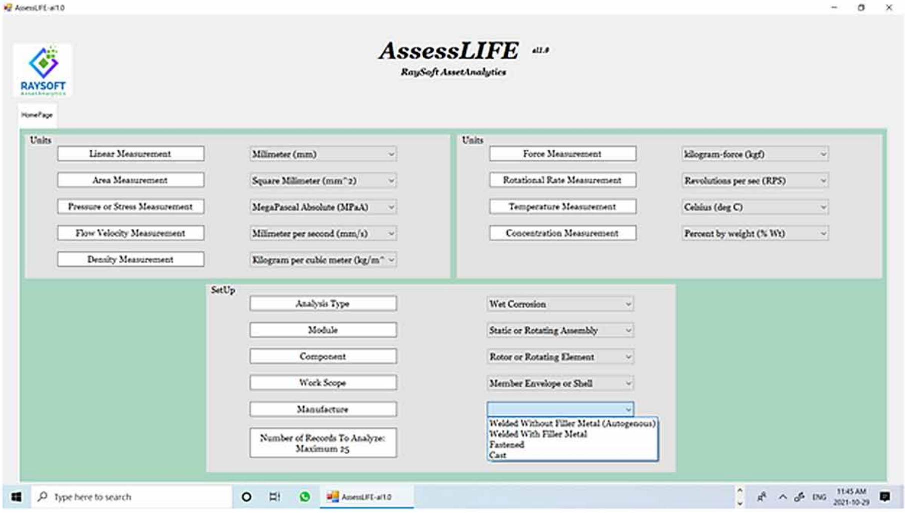
Component: Structural Member

Work Scope: Member Envelope or Shell / Sleeve or Patch on Member Envelope

Manufacture

Number of Records To Analyze: Maximum 25: Please, input Number of Records then pres

Figure 15. AssessLIFE "manufacture" options



AssessLIFE-ai1.0

AssessLIFE ai1.0
RaySoft AssetAnalytics

HomePage

Units

Linear Measurement	Millimeter (mm)
Area Measurement	Square Millimeter (mm^2)
Pressure or Stress Measurement	MegaPascal Absolute (MPaA)
Flow Velocity Measurement	Millimeter per second (mm/s)
Density Measurement	Kilogram per cubic meter (kg/m^

Units

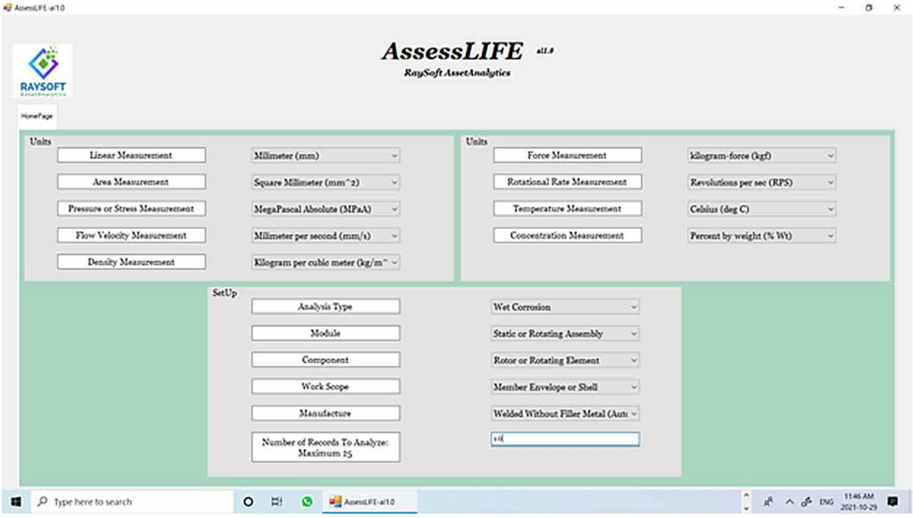
Force Measurement	kilogram-force (kgf)
Rotational Rate Measurement	Revolutions per sec (RPS)
Temperature Measurement	Celsius (deg C)
Concentration Measurement	Percent by weight (% Wt)

SetUp

Analysis Type	Wet Corrosion
Module	Static or Rotating Assembly
Component	Rotor or Rotating Element
Work Scope	Member Envelope or Shell
Manufacture	
Number of Records To Analyze: Maximum 25	

Welded Without Filler Metal (Autogenous)
Welded With Filler Metal
Fastened
Cast

Figure 16. AssessLIFE "number of records to analyze" option



AssessLIFE-ai1.0

AssessLIFE ai1.0
RaySoft AssetAnalytics

HomePage

Units

Linear Measurement	Millimeter (mm)
Area Measurement	Square Millimeter (mm^2)
Pressure or Stress Measurement	MegaPascal Absolute (MPaA)
Flow Velocity Measurement	Millimeter per second (mm/s)
Density Measurement	Kilogram per cubic meter (kg/m^

Units

Force Measurement	kilogram-force (kgf)
Rotational Rate Measurement	Revolutions per sec (RPS)
Temperature Measurement	Celsius (deg C)
Concentration Measurement	Percent by weight (% Wt)

SetUp

Analysis Type	Wet Corrosion
Module	Static or Rotating Assembly
Component	Rotor or Rotating Element
Work Scope	Member Envelope or Shell
Manufacture	Welded Without Filler Metal (Aut
Number of Records To Analyze: Maximum 25	10

The last user configuration box in the "Setup" domain enables users enter the number of records of asset members that the user wishes to analyze. The "Number of Records To Analyze: Maximum 25" data entry box ensures that all the software pages downstream of the HomePage contain the required number of records for all the input fields required by the AssessLIFE software to estimate lifespans and trajectories of degradation drivers.

ASSET MEMBER LIFESPAN ESTIMATION: THEORETICAL BACKGROUND

Each degradation mechanism amongst corrosion, erosion, and fatigue has different sets of mathematic models that an analyst may employ to estimate its degradation rate and, thereafter, the lifespan of the member subjected to that degradation mechanism. In their works, many researchers have either stated mathematic models for asset lifespan estimation (Jones, 1996) (Obi, 2008) (Kececi, 2019) (Edited by Boyer Howard E., 2020, Ninth Printing) (Ebeling, 1997) (Levy, Solid Particle Erosion and Erosion-Corrosion of Materials, 1995) (Okonkwo, 2014) (Elfergani & Abdalla, 2017) or have advanced numerous mathematic formula with which lifespan of asset members subjected to the specified degradation mechanism can be computed (Casesnoves & Surzhenkov, 2017) (Kosa & Goksenli, 2017) (Stack, Chacon-Nava, & Stott, 1995) (Levy & Chik, The Effects of Erodent Composition and Shape on the Erosion of Steel, 1983).

The primary purpose of the AssessLIFE software is to estimate the lifespan of a machine or structure member, given the use conditions of the part or member.

According to Kececi (Kececi, 2019), "Mechanical failure modes can be grouped into two categories: (1) [time independent failure modes or] instant, force or moment dependent, (2) time dependent … It is quite easy to calculate [the lifespan of time independent] failure modes, since there is no uncertainty … For time-dependent failures, it is possible to find the life of a part with experimentation. [Also,] depending on the working conditions of the part, the [time-dependent] mechanical failure modes should be calculated and the life of the part should be known".

AssessLIFE software does not attempt to estimate lifespan for time-independent failure modes. For example, the AssessLIFE software does not estimate the lifespan of a member if cross-section does not contain sufficient material to withstand all forces, stresses, and loadings that the part will be subjected to. Specifically, the AssessLIFE software does not compute lifespan for stress-overload failures from bending, shear, torsion, and buckling. However, for the major time-dependent failure modes, the current version of the AssessLIFE software has the capability to estimate lifespans for the specified time-dependent failure modes, namely, corrosion, erosion, metal fatigue, and corrosion fatigue.

The beneficiaries of asset lifespan generated by the AssessLIFE software include, but are not limited to:

- Managers (who oversee asset related budgets);
- Legal teams (who adjudicate over asset related disputes);

- Insurance teams (who assess risks for insurance coverage);
- Engineers (who implement capital budgets as well as assess assets for safety and productivity);
- Fabricators (who implement engineering designs);
- Inspectors (who assess and report on asset status).

The pain points which the AssessLIFE software addresses with solutions include, but are not limited to:

- Asset safety and health assessment (the AssessLIFE software assesses physical asset degradation over time and generates status report);
- Production loss (the AssessLIFE software ensures that assets are built from the most appropriate alloys and welds. Appropriate selection of alloys and welds facilitates continuous production);
- Maintenance cost overruns (the AssessLIFE software generates asset inspection time frames ahead of possible time-dependent failures. This information facilitates pro-active remedial actions);
- Legal assessment (the AssessLIFE software computes asset lifespan based on the alloy of construction and ambient exposure environments which inform legal teams if the appropriate early-phase decisions were made);
- Insurability assessments (the AssessLIFE software computes lifespans and remaining life of metallic physical assets which enable insurers quantify asset insurability);
- Engineering decision-making (the AssessLIFE software computes and generates rates of degradation drivers and lifespans to ensure that the most appropriate engineering decisions are made);
- Fabrication decision-making (the AssessLIFE software proposes to fabricators information on the most appropriate welds for the exposure environment);
- Inspection preparation (the AsssessLIFE software provides inspectors with possible degrading mechanisms and expected physical damage features so that the most appropriate inspection tools and techniques can be selected).

In summary, the AssessLIFE software is a solution platform that analyzes and reveals (at design time or at operating time) if the industrial physical asset made of metals, alloys, and welds can survive their exposure or ambient conditions. The software also reveals when time-dependent pre-mature failure is likely to occur. The AssessLIFE software aims to provide asset information for better financial and technical decision-making by managers, engineers, legal teams, insurance teams, fabricators, and inspectors. Furthermore, the AssesLIFE software can generate great financial and safety benefits for all stakeholders.

In the current version of the AssessLife software, asset degradation lifespans can only be treated under a specified degradation mechanism comprising corrosion, erosion, or fatigue. Each of these degradation mechanisms is unique and proceeds according to its own processes that eventually culminates in the failure of the part, member, or assembly. Corrosion, erosion, or fatigue is influenced by unique sets of inputs (emanating from either or a combination of the design engineer, operator, field conditions, or environmental conditions) and each of the mechanisms is driven to failure by unique sets of intermediate variables.

Modeling Lipespan Under Corrosion Degradation Mechanism

To model the lifespan of an asset member subjected to corrosion degradation, it is imperative to analyze the corrosion processes defined by the specific sub-mechanism that drives the corrosion damage. The sub-mechanisms of corrosion damage include, but are not limited to (Cicek, 2013):

1. General corrosion (typified by broad metal loss on the surface of the asset or alloy);
2. Pitting corrosion (depicted by perforation of the asset or alloy);
3. Crevice corrosion (depicted by localized aggressive attack on metals in close contact with corrosive stagnant fluid trapped between them);
4. Galvanic corrosion (exemplified by loss within two dissimilar regions of a structure of which metal loss occurs on one region of structure (the anode or active region) which is in electrical or physical contact with the protected region of the structure (the cathode or passive region));
5. Stress Corrosion Cracking (typified by cracks initiated by a combined action of stress and corrosion);
6. Intergranular corrosion (characterized by corrosion of grain boundaries leading to a compromised grain structure);
7. Erosion Corrosion (depicted as metal loss in areas of high fluid velocity or solid-particle action):
8. Caustic Embrittlement (characterized by cracks initiated by very high pH)
9. Hydrogen Embrittlement (exemplified by cracks and fracture initiated by gas pressure when atomic hydrogen infiltrated into the metal crystal combines to form vastly higher-volume molecular hydrogen);
10. Stray-current corrosion (depicted by metal loss which occurs when current flows between unprotected assets and cathodically protected assets);
11. Microbial or biocorrosion (corrosion damage that is caused by microbes and other living organisms);

12. Corrosion Fatigue (typified by damage resulting from the combined action of corrosion and fatigue resulting in accelerated failure rate)

Several researchers (Obi, 2008, p. 15) (Jones, 1996, p. 34) showed that the rate of degradation propagated by <u>general corrosion</u> can be modeled by

$$CR\left(\frac{mm}{yr}\right)=\frac{87.6W}{DAt} \tag{1}$$

where 87.6 is a constant, *W* is weight loss in mg, *D* is density in g/cm^3, *A* is surface area in cm^2, and *t* is time in hours.

Consequently, the lifespan of the member with thickness, $T\left(mm\right)$ is

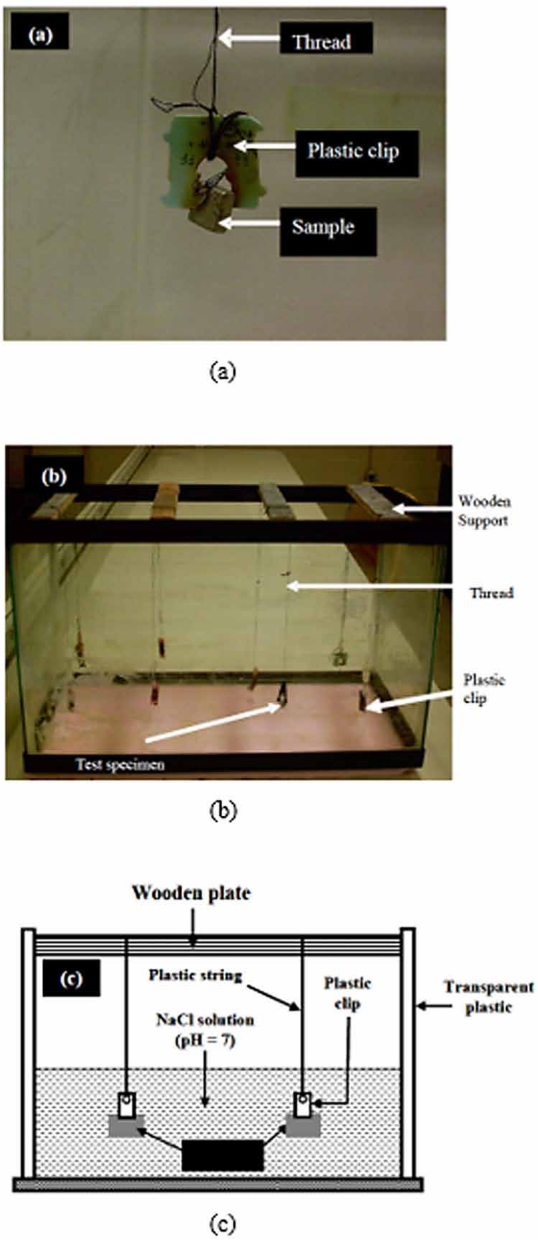
$$Lifespan\left(yr\right)=\frac{T\left(mm\right)}{CR\left(\frac{mm}{yr}\right)} \tag{2}$$

Subir (Subir, 2010) proposed an alternative method to estimate the corrosion rate of mild steel in water using interpolation, regression, and factorial design. Furthermore, Soares (Soares, Garbatov, & Zayed, 2011) modeled the individual effects of the different environmental or ambient parameters that drive the uniform corrosion rate of carbon steel alloy. The efforts of these researchers show that there are various pathways by which the degradation process can be quantified. The goal is always to represent complex natural and physical processes using representative mathematical models which deliver outcomes that mimic reality as closely as possible. Figure 17 shows laboratory setup with which Obi (Obi, 2008) modeled the general corrosion rate of alloys.

Beside general corrosion, to model <u>pitting corrosion</u>, the American Society for Testing and Materials (ASTM International, 2003) provided the following insights on a key parameter -- the critical pitting temperature (CPT) -- that governs the initiation and propagation of pits on an alloy. The critical pitting temperature is an experimentally and statistically determined temperature above which pits initiate on an alloy. The critical pitting temperature (CPT) of an alloy is modeled by:

$$CPT(^{o}C)=\left(2.5\times\%Cr\right)+\left(7.6\times\%Mo\right)+\left(31.9\times\%N\right)-41.0 \tag{3}$$

Figure 17. Weight-loss corrosion test apparatus: (a) specimen suspended by plastic clip and thread (b) immersion corrosion cell (c) a schematic of the immersion corrosion cell.



(a)

(b)

(c)

where %Cr is weight percent content of chromium in the alloy, %Mo is the weight percent content of molybdenum in the alloy, and %N is the weight percent content of nitrogen in the alloy. Hence, in the presence of chlorides (or other corrodents), when the exposure, ambient, or operating temperature is greater than the CPT, the alloy is susceptible to pitting corrosion attack. Additional computations can be performed with the critical pitting temperature (CPT) parameter to arrive at the lifespan of the alloy subjected to pitting corrosion attack.

Similar to pitting corrosion, the American Society for Testing and Materials (ASTM) also provide insights into modeling crevice corrosion. Crevice corrosion can be modeled via the determination of the critical crevice temperature (CCT). The critical crevice temperature (CCT) is an experimentally and statistically determined temperature above which crevice corrosion attack on an alloy initiates and progresses. Hence, in the presence of chlorides (or other corrodents) when the exposure, ambient, or operating temperature is greater than the CCT, the alloy is susceptible to crevice corrosion attack – if a stagnant fluid is trapped between two adjacent narrowly separated surfaces of which one is a susceptible metal or alloy. Additional computations can be performed with the critical crevice temperature (CCT) to arrive at the lifespan of the alloy subjected to crevice corrosion attack. The critical crevice temperature (CCT) of an alloy is modeled by:

$$CCT(^{o}C) = \left(3.2 \times \%Cr\right) + \left(7.6 \times \%Mo\right) + \left(10.5 \times \%N\right) - 81 \tag{4}$$

where %Cr is weight percent content of chromium in the alloy, %Mo is the weight percent content of molybdenum in the alloy, and %N is the weight percent content of nitrogen in the alloy. Additional computations can be performed with the

Figure 18. The ECM8 electrochemical multiplexer system equipped with a PCI4 potentiostat.

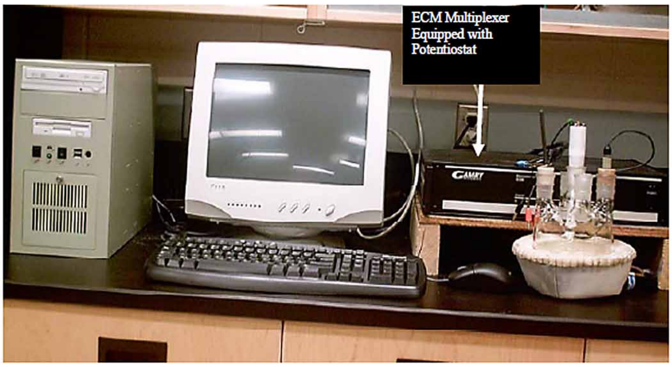


Figure 19. Exploded view of the working electrode holder.

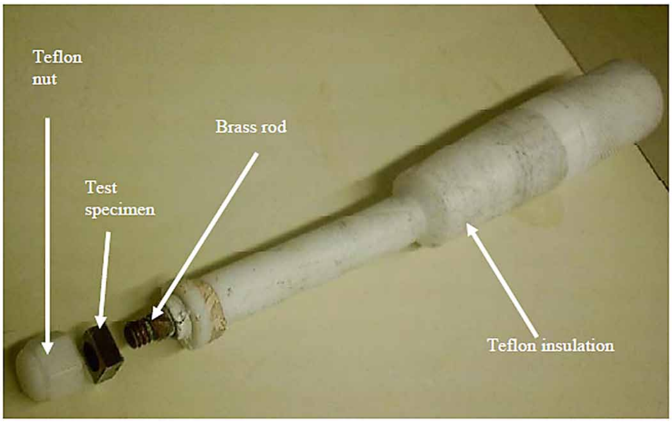
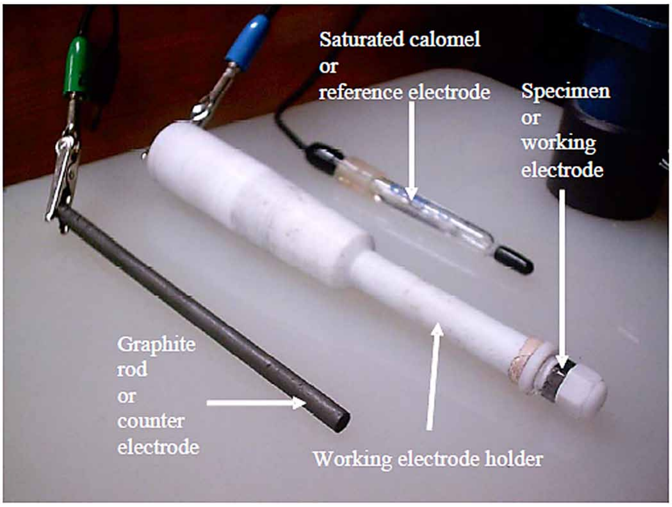


Figure 20. Working electrode, reference electrode (SCE) and graphite counter electrode used in the study.


Saturated calomel or reference electrode
Specimen or working electrode
Graphite rod or counter electrode
Working electrode holder

critical crevice temperature (CCT) to arrive at the lifespan of the alloy subjected to crevice corrosion attack. Figure 18, Figure 19, Figure 20, Figure 21, and Figure 22 show laboratory devices with which Obi (Obi, 2008) determined the critical pitting temperature and critical crevice temperature, respectively, of alloys.

Welds are also subjected to similar conditions as alloys and can also suffer general, pitting, and crevice corrosion attack (Lippold, 2015) (Dupont, Lippold, & Kiser, 2009) (Kotecki & Lippold, 2005) (Phillips, 2016). The metallurgy of welds

Figure 21. A schematic diagram of the working electrode and holder assembly.

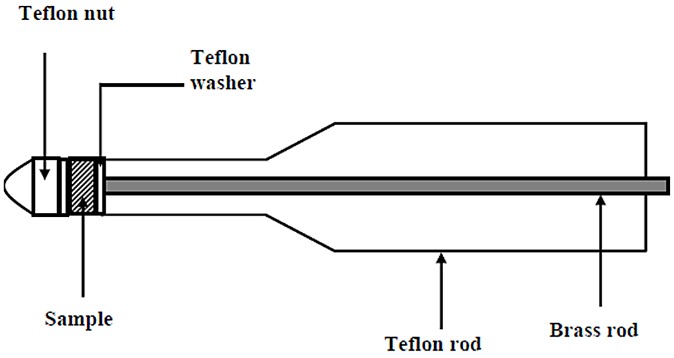
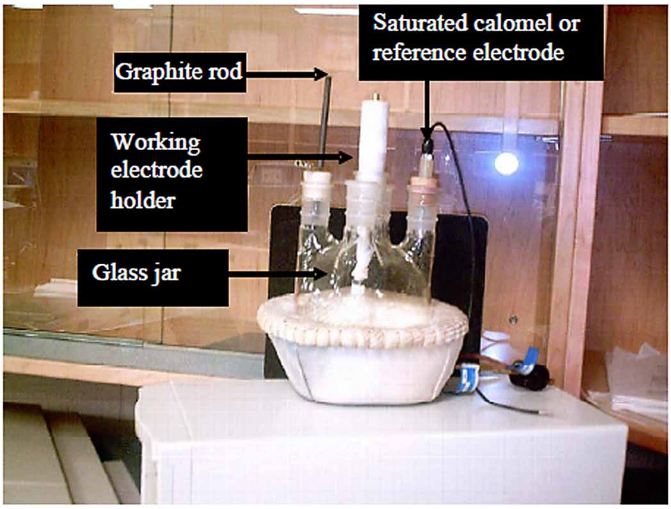


Figure 22. Corrosion cell and electrodes used in electrochemical measurements.



is more complex than that of alloys since welds are typically air-cooled to room temperature at cooling rates much faster than those of alloys. Alloys are typically control-cooled in furnaces to room temperature. The rapid cooling rates of welds can create intermediate phases – and even deleterious phases – that can actively facilitate different types of corrosion attack. Furthermore, the physical, mechanical, and chemical integrity of welds are influenced by additional factors such as weld current and voltage, travel speed, welding gases, contamination of weld surfaces, and weld defects. These factors can complicate further the susceptibility of welds to corrosion attack and the assessment of welds for adequacy and integrity. The AssessLIFE software estimates the corrosion lifespan of welds using varying modification of Equations 1,2,3,4.

Modeling Lifespan Under Erosion Degradation Mechanism

Erosion can be described as the continuous removal of tiny pieces of the target alloy by either a rapidly flowing turbulent fluid or by solid particles transported by the fluid. Many researchers (Okonkwo, 2014) (Levy, 1995) (Casesnoves & Surzhenkov, 2017) (Levy & Chik, 1983) (Kosa & Goksenli, 2017) (Stack, Chacon-Nava, & Stott, 1995) modeled and advanced mathematical formulation of the degradation caused by erosion. A model of the erosion attack on alloys was postulated via the work of Wada et al (Wada & Watanalm, 1987) and (Okonkwo, 2014) as

$$E\alpha\left(\frac{H_t}{H_p}\right)^w \tag{5}$$

where E is the erosion rate, H_t is the target material hardness, H_p is the eroding particle material hardness, and w is an empirically determined exponent. The model accounted for the importance of alloy hardness of the both the target material and the stream-borne solid particles. However, it failed to account for the importance of stream velocity. Hutchings' mathematical model (Hutchings, 1992) included the effect of stream velocity and target material density.

$$E = \frac{kpv^2}{2H} \tag{6}$$

where E is the mass of material eroded, v is the mean solid-particle velocity, H is the hardness of the erodents, p is the density of target material, and k is the wear coefficient. Hutching (Hutchings, 1992) had earlier formulated Equation 6 to include the impact angle of the stream solid-particles represented as alpha:

$$E = \frac{kp\left(v\sin\alpha\right)^{2.5}}{H\left(s\right)} \tag{7}$$

The research study presented by Levy (Levy, 1995) show numerous mathematic models that apply to erosion damage and cover the influences of particle shape, attack angle, particle strength and density, particle velocity, as well as target material hardness and density. The relevant mathematical models can be employed to compute the erosion rates on alloys. With the erosion rates computed, the lifespan of an alloy of thickness, $T\left(mm\right)$ under primarily erosion attack can be estimated by the model

$$Lifespan\left(yr\right)=\frac{T\left(mm\right)}{E\left(\frac{mm}{yr}\right)} \tag{8}$$

Modeling Lifespan Under Fatigue Degradation Mechanism

Fatigue is the failure mode that can occur when an alloy or an asset member is subjected to fluctuating or alternating stresses, forces, or loadings, which drive the alloy or asset member to initiate and propagate cracks that result in fracture of alloy or asset member. Fatigue can weaken an alloy or asset member when the member is subjected to back-and-forth loading. Stress concentration created by notches, tight radii, defects in the alloy or asset member and other features that raise stress levels (or stress concentration drivers) in the member can accelerate fatigue failure. The number of cycles to failure or lifespan of an alloy or asset member, especially when stress concentration drivers are present, can be modeled by the strain life equation (Kececi, 2019) (Edited by Boyer Howard E., 2020, Ninth Printing):

$$\frac{\Delta\varepsilon}{2}=\frac{\Delta\varepsilon_e}{2}+\frac{\Delta\varepsilon_p}{2} \tag{9}$$

where $\Delta\varepsilon_e$ is the elastic strain amplitude and $\Delta\varepsilon_p$ is the plastic strain amplitude.

According to the Coffin-Manson formula presented in the works of Kececi (Kececi, 2019) and Boyer (Edited by Boyer Howard E., 2020, Ninth Printing)

$$\frac{\Delta\varepsilon_p}{2}=\varepsilon_f\left(2N_f\right)^c \tag{10}$$

where ε_p is the plastic strain amplitude, ε_f is the fatigue ductility coefficient, N_f is the number of cycles before failure, and *c* is the Cofflin's exponent.

Furthermore, as presented in the same works Kececi (Kececi, 2019) and Boyer (Edited by Boyer Howard E., 2020, Ninth Printing), the number of cycles to failure or lifespan can be extended by applying the Basquin formula:

$$\frac{\Delta\varepsilon_e}{2}\sim\frac{\Delta\sigma}{2}=\sigma_f\left(2N_f\right)^b \tag{11}$$

where $\frac{\Delta\sigma}{2}$ is the stress amplitude, N_f is the number of cycles before failure, *b* is the Basquin's exponent, and σ_f is the fatigue strength coefficient.
For one-dimensional loading,

$$\frac{\Delta\varepsilon_e}{2} = \frac{\Delta\sigma}{2E} = \frac{\sigma_a}{E} \tag{12}$$

where *E* is Youngs Modulus, σ_a is stress amplitude, and $\Delta\sigma$ is the stress range.
Substituting equations 9,10, and 11 into equation 12

$$\frac{\Delta\varepsilon}{2} = \frac{\sigma_f}{E}\left(2N_f\right)^b + \varepsilon_f\left(2N_f\right)^c \tag{13}$$

The number of cycles to failure or the lifespan of an alloy or asset member subjected to fatigue load can be estimated as:

$$2N_f = \left(\frac{\varepsilon_f E}{\sigma_f}\right)^{\frac{1}{(b-c)}} \tag{14}$$

Based on fatigue loading of an asset member, the AssessLIFE software models and estimates the lifespan of asset members subjected to the fatigue degradation process. Since welds and discontinuities (that is, areas of high stress concentration resulting from typically notches, tight-radii, transitions, etc) are particularly vulnerable to the initiation events of fatigue failure, the AssessLIFE software can discriminate between the fatigue vulnerabilities of different types of welds and different discontinuity-features employed during the manufacture of asset members into machine or structural assemblies. In addition to estimating the lifespan of plain members subjected to fatigue loading, the AssessLIFE software also analyzes the contribution of the different weld types and discontinuity-features to both the possibility of occurrence fatigue failure and to lifespan of the considered asset member.

Modeling Cumulative Damage and Remaining Lifespan of an Alloy or Asset Member

Some researchers (Ebeling, 1997) (Ertas, 2012) have documented mathematic models that track the progress of cumulative damage on structures. As presented by Ebeling (Ebeling, 1997), “if the damage rate depends only on the amount of damage and not on any past history”, the progressive cumulative damage severity can be generalized by Miner’s rule:

$$\sum_{i=1}^{n} \frac{t_i}{L_i} = 1 \tag{15}$$

where t_i = the amount of time at stress or damage level *i* and L_i is the expected lifetime at stress or damage level *i*.

Using Miner’s rule, the remaining lifespan of an asset can be estimated when two or more stress or damage levels are considered via the model:

$$\frac{t_1}{L_1} + \frac{t_2}{L_2} = 1 \tag{16}$$

where t_1 and t_2 = the amount of time at stress or damage level *1 & 2* respectively and L_1 & L_2 is the expected lifetime at stress or damage level *1 & 2*, respectively. On further simplification,

$$t_2 = L_2 - \frac{L_2}{L_1} t_1 \tag{17}$$

If the lifespan at damage level 1 (L_i) is known and the exposure times of the asset at damage level 1 and 2 (t_1 and t_2) are known, the remaining life L_2 of asset member or alloy subjected to cumulative damage is estimated by

$$L_2 = \frac{L_2}{L_1} t_1 + t_2 \tag{18}$$

Using similar mathematic models, the AssessLIFE software has the capability to estimate the remaining life of an alloy or asset member. The remaining life computation is a particularly beneficial service provided by the AssessLIFE software. The capability to compute the remaining lifespan of asset members or alloys is coupled to the software’s capability to determine the lifespan of members under different degradation mechanisms such as corrosion, erosion, and fatigue. Further to the determination of lifespan of an alloy or asset member under different degradation mechanisms and exposure conditions, the software can thereafter apply these lifespans in the remaining life modeling and analysis (Equations 15,16,17, and 18) to progressively cumulative damage done by the antecedent damage mechanism, and estimate the remaining lifespan of the exposed asset member or alloy.

OVERVIEW OF THE ASSESSLIFE SOFTWARE

The AssessLIFE software models many practical alloy and weld selection decision-making tasks. **Modeling** attempts to transfer physical asset attributes and user data into mathematic attributes that can be manipulated, transformed, x-rayed, diagnosed, assessed, dissected, and synthesized using the myriad mathematical principles, theorems, theories, concepts, and formulations that have been collated since the dawn of science and technology.

The AssessLIFE software integrates the concepts in and from many engineering fields and employs each field's specific mathematical models to analyze the degradation processes with the domain of the specific engineering field. The engineering disciplines include mechanical, electrical, electronic, metallurgical, materials, process, chemical, welding, and corrosion engineering. **Integrating** involves synthesizing related or connected engineering principles, theorems, theories, concepts, and formulations from the different engineering disciplines with which to solve multi-disciplinary engineering problems and provide multi-discipline engineering solutions.

The AssesLIFE software performs **automation of alloy and asset degradation to estimate asset lifespan and degradation drivers analytics** by using tested and proven scientific analytical computations, forecasting, prediction, and analytics. By automating the process of degradation using mathematical models, and subsequently, estimating the asset-member lifespans as well as other vital degradation statistics, the AssessLIFE software can assess the health status of assets and their members exposed to intended service conditions or exposed to unexpected or rare upset conditions.

An asset is pictured, depicted, or represented as an entity that is built up from multiple assemblies – either from welded assemblies (or weldment) or from fastened assemblies – as shown in Figure 23 and Figure 24. The AssessLIFE software contains more than sixty different assembly scenarios.

The butt-welded assembly (Figure 23) and/or the fillet-welded assembly (Figure 24) can be interlaced multiple times to constitute industrial physical assets such as tanks, pipings, evaporators, crystallizers, pressure vessels, compactors, screens, condensers, boilers, etc. An asset may be composed of one identical assembly or many dissimilar assemblies. Each assembly can be analyzed by the AssessLIFE software to estimate its lifespan and other vital health statistics. As shown in, with

Figure 23. A butt weld assembly.

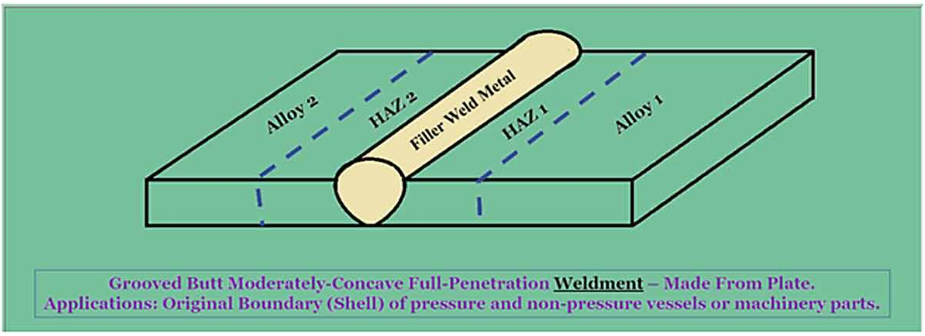
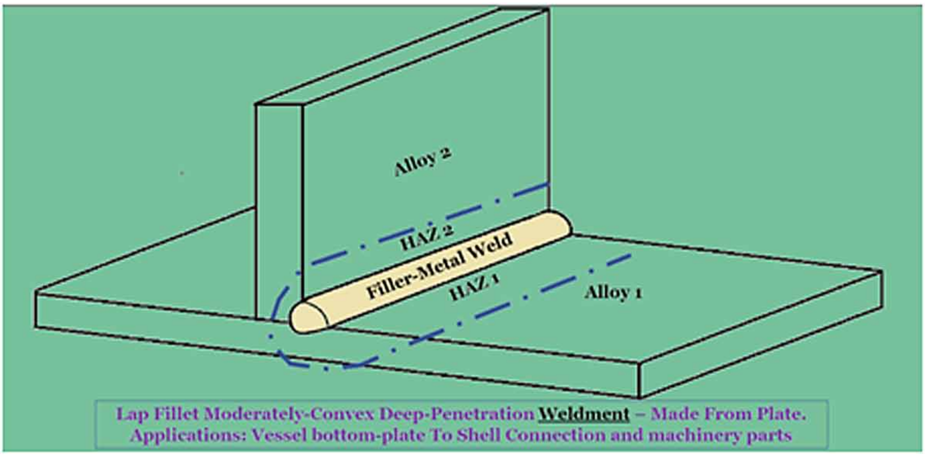

Alloy 2
HAZ 2
Filler Weld Metal
HAZ 1
Alloy 1
Grooved Butt Moderately-Concave Full-Penetration Weldment – Made From Plate.
Applications: Original Boundary (Shell) of pressure and non-pressure vessels or machinery parts.

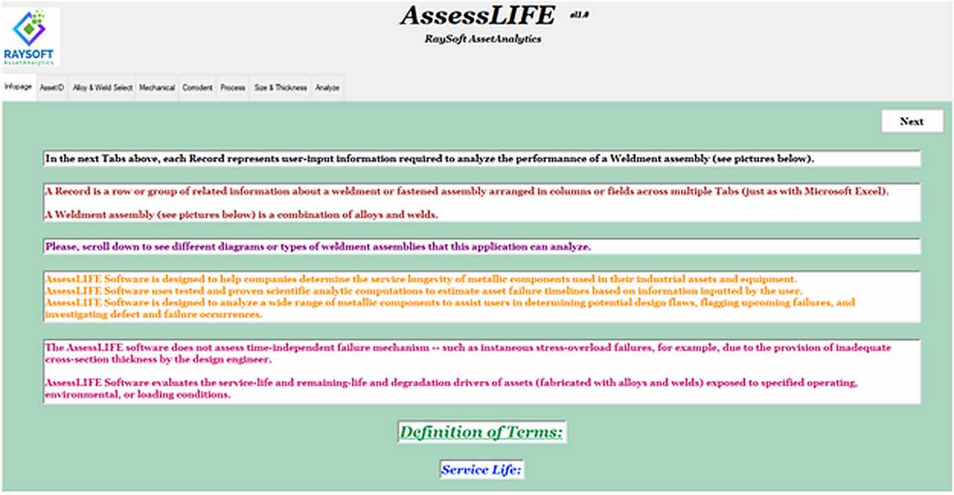
Figure 24. A fillet weld assembly.


Alloy 2
HAZ 2
Filler-Metal Weld
HAZ 1
Alloy 1
Lap Fillet Moderately-Convex Deep-Penetration Weldment – Made From Plate.
Applications: Vessel bottom-plate To Shell Connection and machinery parts

the AssessLIFE software different alloys can be assigned to “Alloy 1” and “Alloy 2”. Thereafter, the software user can input service conditions. The AssessLIFE software estimates the lifespan of the alloy and its other vital health statistics using the input data. Similarly, different weld filler metals can be assigned to “Filler-Metal Weld” along with input service conditions. With these inputs, the AssessLIFE software can also estimate the lifespan of the different regions of the weld. Consequently, the AssessLIFE software can determine the lifespan of a user defined weldment.

For analysis via the “wet corrosion” degradation mechanism, the AssessLIFE software commences with an information window called “InfoPage” as shown in Figure 25. The “InfoPage” defines all relevant terms employed in the software. This window also displays the pictures of the assembly configuration selected for analysis. The goal of the “InfoPage” is to enhance the user-friendliness of the software. For

Figure 25. The AsessLIFE software: "InfoPage" read-only window.



In the next Tabs above, each Record represents user-input information required to analyze the performannce of a Weldment assembly (see pictures below).

A Record is a row or group of related information about a weldment or fastened assembly arranged in columns or fields across multiple Tabs (just as with Microsoft Excel).

A Weldment assembly (see pictures below) is a combination of alloys and welds.

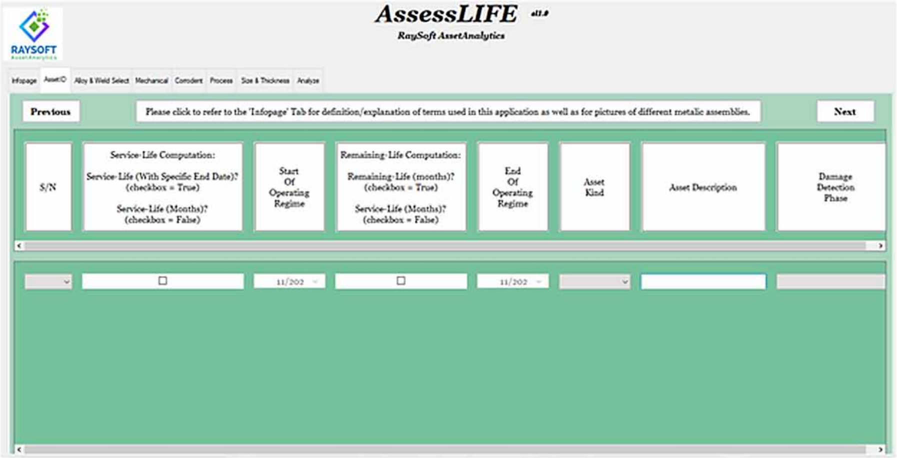
Please, scroll down to see different diagrams or types of weldment assemblies that this application can analyze.

AssessLIFE Software is designed to help companies determine the service longevity of metallic components used in their industrial assets and equipment.
AssessLIFE Software uses tested and proven scientific analytic computations to estimate asset failure timelines based on information inputted by the user.
AssessLIFE Software is designed to analyze a wide range of metallic components to assist users in determining potential design flaws, flagging upcoming failures, and investigating defect and failure occurrences.

The AssessLIFE software does not assess time-independent failure mechanism -- such as instaneous stress-overload failures, for example, due to the provision of inadequate cross-section thickness by the design engineer.

AssessLIFE Software evaluates the service-life and remaining-life and degradation drivers of assets (fabricated with alloys and welds) exposed to specified operating, environmental, or loading conditions.

Figure 26. The AssessLIFE software: "Asset ID" input window.

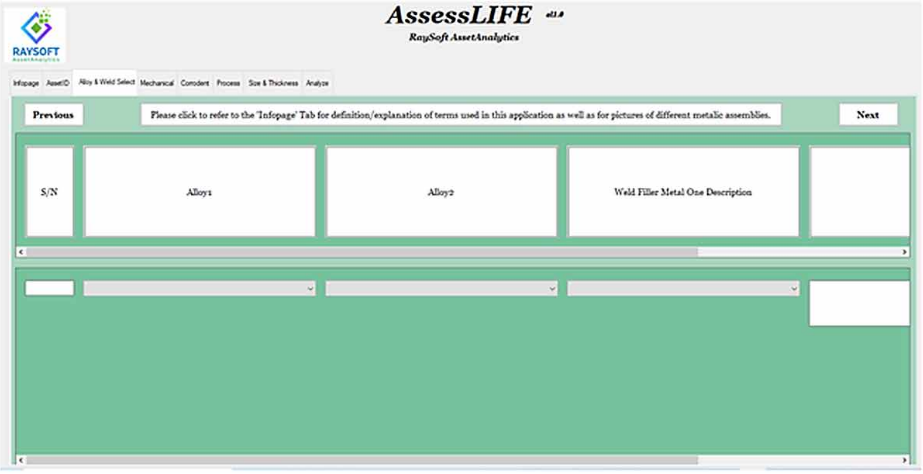


Please click to refer to the 'Infopage' Tab for definition/explanation of terms used in this application as well as for pictures of different metalic assemblies.

S/N	Service-Life Computation: Service-Life (With Specific End Date)? (checkbox = True) Service-Life (Months)? (checkbox = False)	Start Of Operating Regime	Remaining-Life Computation: Remaining-Life (months)? (checkbox = True) Service-Life (Months)? (checkbox = False)	End Of Operating Regime	Asset Kind	Asset Description	Damage Detection Phase
	☐	11/202	☐	11/202			

the "wet corrosion" analysis type, the next window of the software, the "Asset ID" (Figure 26), contains asset identification information. This page enables the user input identification information for each asset to be analyzed. Subsequently, the user selects alloys and welds in the "Alloy and Welds Select" window (Figure 27). The alloy configuration box is a dropdown box which lists more than 400 different alloys that are selectable from AssessLIFE version 1.0. Future versions of the AssessLIFE software will add many more alloys to the current list of alloys. Similarly, the weld

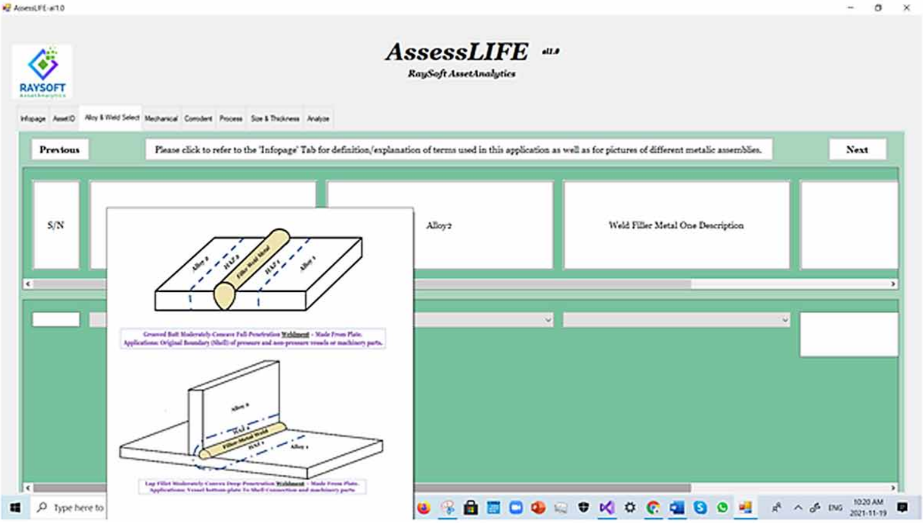
Figure 27. The AssessLIFE software: "Alloy and Weld Select"input window.



Please click to refer to the 'Infopage' Tab for definition/explanation of terms used in this application as well as for pictures of different metalic assemblies.

S/N	Alloy1	Alloy2	Weld Filler Metal One Description	

Figure 28. The AssessLIFE software: "Alloy and Weld Select" input window with popup of assembly assessed.



Please click to refer to the 'Infopage' Tab for definition/explanation of terms used in this application as well as for pictures of different metalic assemblies.

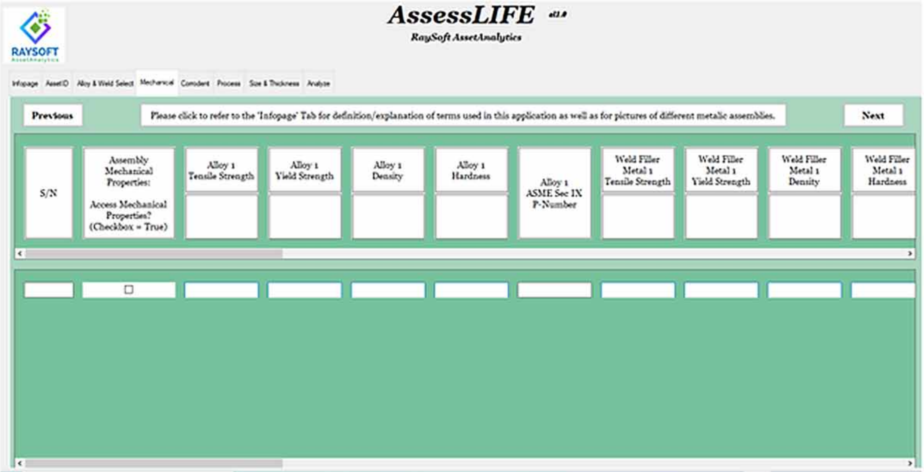
S/N		Alloy2	Weld Filler Metal One Description	

Grooved Butt Moderately Concave Full Penetration Weldment - Made From Plate.
Applications: Original Boundary (Shell) of pressure and non-pressure vessels or machinery parts.

Lap Fillet Moderately Convex Deep Penetration Weldment - Made From Plate.
Applications: Vessel bottom plate To Shell Connection and machinery parts

filler metal configuration box is a dropdown list with more than 350 different filler metal welds that are selected from AssessLIFE version 1.0. For both the alloys and the welds, the classes of materials covered in this version of the software include low carbon steels, medium carbon steels, chrome-moly steels, austentic stainless steels, superaustentic steels, duplex stainless steels, superduplex stainless steels,

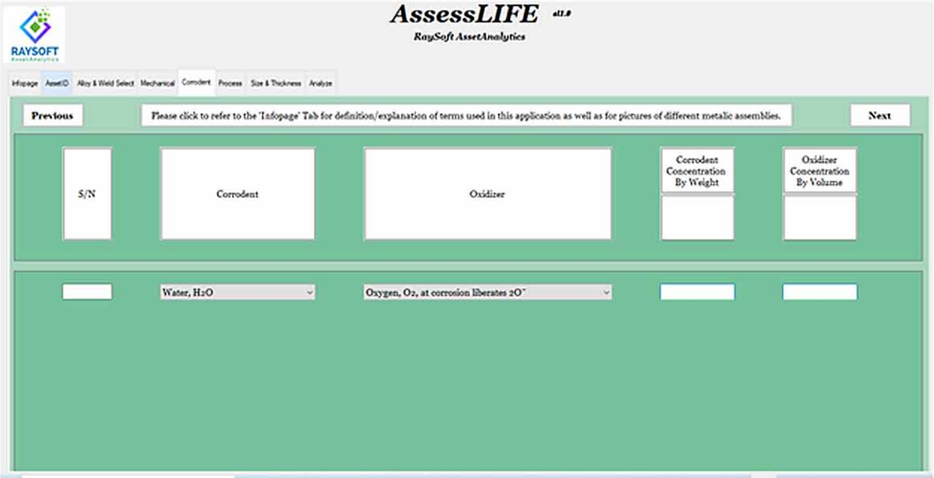
Figure 29. The AssessLIFE software: "mechanical" properties display window.



Please click to refer to the 'Infopage' Tab for definition/explanation of terms used in this application as well as for pictures of different metalic assemblies.

S/N	Assembly Mechanical Properties: Access Mechanical Properties? (Checkbox = True)	Alloy 1 Tensile Strength	Alloy 1 Yield Strength	Alloy 1 Density	Alloy 1 Hardness	Alloy 1 ASME Sec IX P-Number	Weld Filler Metal 1 Tensile Strength	Weld Filler Metal 1 Yield Strength	Weld Filler Metal 1 Density	Weld Filler Metal 1 Hardness
	□									

Figure 30. The AssessLIFE software: "corrodent" properties input window.

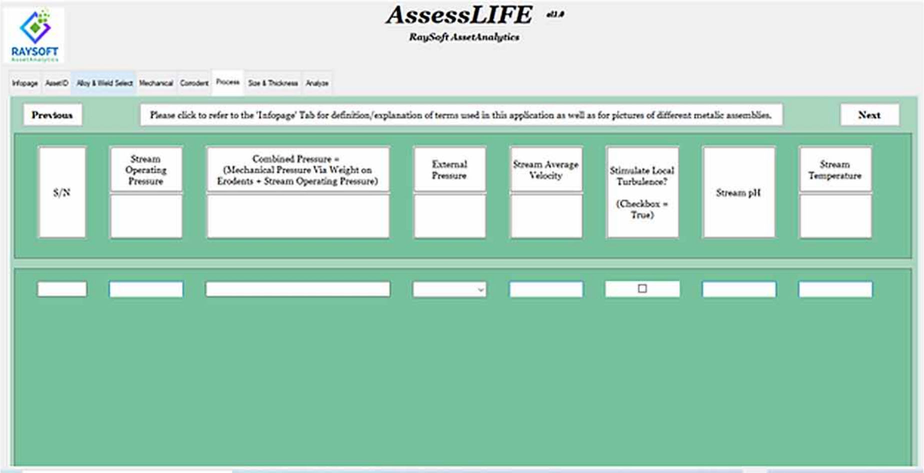


Please click to refer to the 'Infopage' Tab for definition/explanation of terms used in this application as well as for pictures of different metalic assemblies.

S/N	Corrodent	Oxidizer	Corrodent Concentration By Weight	Oxidizer Concentration By Volume
	Water, H_2O	Oxygen, O_2, at corrosion liberates $2O^-$		

nickel-chromium alloys, nickel-molybdenum alloys, nickel-chromium-molybdenum alloys, nickel-copper alloys, etc. Figure 28 shows another feature that enhances the user-friendliness of the AssessLIFE software. On mouseover the alloy configuration box, a popup of the assembly selected for analysis is displayed. This feature enables the user visualize the assembly as they enter the alloy and weld user data.

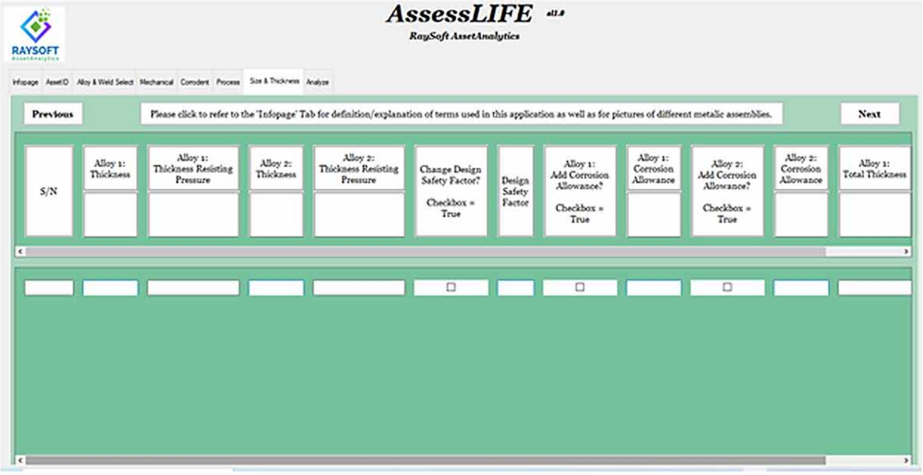
Figure 31. The AssessLIFE software: "process" properties input window.



Please click to refer to the 'Infopage' Tab for definition/explanation of terms used in this application as well as for pictures of different metalic assemblies.

S/N	Stream Operating Pressure	Combined Pressure = (Mechanical Pressure Via Weight on Erodents + Stream Operating Pressure)	External Pressure	Stream Average Velocity	Stimulate Local Turbulence? (Checkbox = True)	Stream pH	Stream Temperature
					□		

Figure 32. The AssessLIFE software: "size & thickness" input window.

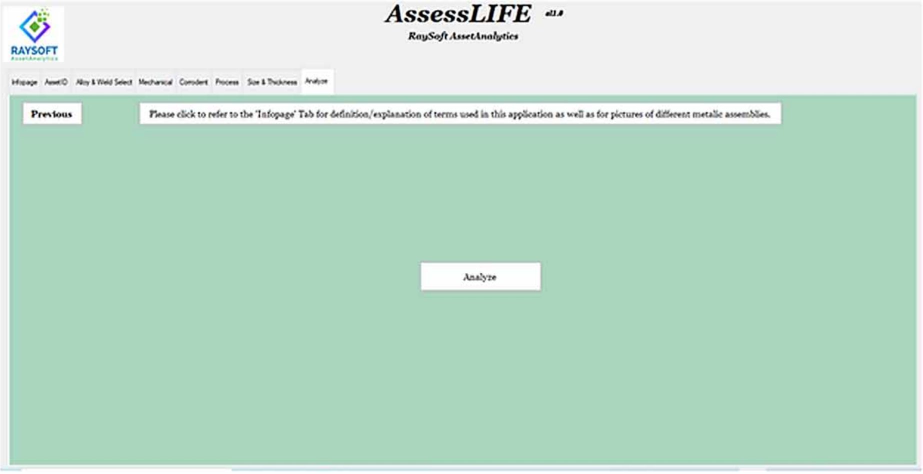


Please click to refer to the 'Infopage' Tab for definition/explanation of terms used in this application as well as for pictures of different metalic assemblies.

S/N	Alloy 1: Thickness	Alloy 1: Thickness Resisting Pressure	Alloy 2: Thickness	Alloy 2: Thickness Resisting Pressure	Change Design Safety Factor? Checkbox = True	Design Safety Factor	Alloy 1: Add Corrosion Allowance? Checkbox = True	Alloy 1: Corrosion Allowance	Alloy 2: Add Corrosion Allowance? Checkbox = True	Alloy 2: Corrosion Allowance	Alloy 1: Total Thickness
					□		□		□		

The selection of an alloy or weld filler metal will call out its mechanical properties in Figure 29. The user can edit the mechanical properties of the alloy or weld filler metal to account for real-life processes which alter the mechanical properties of the materials such as heat treatment and other metal working processes. While the mechanical properties of alloys and welds may not generate significant contributions to corrosion degradation, which proceeds via chemical means, some mechanical properties do contribute significantly to erosion, metal fatigue, and corrosion fatigue degradation processes. As shown in Figure 30, The "Corrodent"

Figure 33. The AssessLIFE software: "analyze" command window.



Please click to refer to the 'Infopage' Tab for definition/explanation of terms used in this application as well as for pictures of different metalic assemblies.

input window succeeds the mechanical page. In this page in version 1.0 of the AssessLIFE software, the corrodent dropdown list contains steam, water, chloride solution, hydrochloric acid, hydrobromic acid, hydrogen sulfide, sulfuric acid, nitric acid, phosphoric acid, chromic acid, acetic acid, and formic acid. Furthermore, the oxidizer or accelerant dropdown list includes oxygen, ozone, fluorine, bromine, iodine, hypocrite, chlorate, Sulphur dioxide, dichromate, permanganate, manganate, ferric chloride, and ferrous chloride.

Figure 31 shows that the "process" window succeeds the "corrodent" page. In the process page, the user inputs the service process parameters such as fluid velocity, temperature, pH, and pressure. The last input window in the software for the "wet corrosion" degradation mechanism is the "size & thicknesses" window. Here, the user enters the physical dimension of the asset or assembly. The next window (Figure 33) or the "Analyze" window contains the "Analyze" button with which the software analysis is initiated.

SIMULATED RESULTS AND ANALYSIS

The AssessLIFE software can simulate many practical real-life degradation scenarios. Two scenarios are be demonstrated.

AssessLIFE Software: The Effect of Oxygen on the Uniform Corrosion of Carbon Steels in Chloride Solution

Table 1 shows the parameters with which to simulate the wet corrosion degradation of a carbon steel alloy in chloride solution. Alloy “A” is identical to Alloy “B”. They are subjected to identical service conditions with the exception of the oxygen exposure conditions. The AssessLIFE software simulates the degradation via the “wet corrosion” degradation mechanisms and generates the results shown in Figure 34 and Figure 35.

Table 1. Parameters for carbon steel corrosion simulation

Carbon Steel Alloy	Oxygen (ppb)	Temperature (C)	pH	Flow Velocity (m/s)	Chloride Conc (wt %)	Thickness (mm)
A	20	50	8	1.0	3	9.5
B	15000	50	8	1.0	3	9.5

From Table 1, it can be seen that the identical carbon steel alloys “A” & “B” are exposed to identical service conditions – except for the oxygen concentration exposure difference between the two alloys. Carbon steel alloy “A” was exposed to 20 ppb in contrast to 1500 ppb to which carbon steel alloy “B” was exposed to. Figure 34 shows that this difference in oxygen exposure concentration reduced the expected lifespan of carbon steel alloy “B” from 23 to 2 years – more than 90% reduction in the service life of carbon steel. Hence, the AssessLIFE software provides great safety, technical, and financial benefits by providing the lifespan analytics and other high-value analytics for its users and enhance their decision-making capabilities. Similarly, Figure 35 and Figure 36 provide analytics on the degradation of the carbon steels alloy “A” and alloy “B”. The analytics from Figure 35 and Figure 36 show that an increase from 20 ppb oxygen exposure to 1500 ppb (or 15 ppm) increased the oxygen contribution to the corrosion rate of carbon steel alloy from 0.01 mm/year degradation rate to 2 mm/year degradation rate. Furthermore, the increase in exposure oxygen generated an increase in the total corrosion rate from 0.4 mm/year to 2.55 mm/year – which is a 500% increase in the degradation rate of the carbon steel alloy. Similar degradation rates were generated by multiple researchers who investigated the corrosion of carbon steel alloys exposure to similar environmental conditions (Do & Roy, 1994) (Priyotomo, Lutviasari, & Siska, 2017)

Figure 34. AssessLIFE software: simulated lifespan (in years) of carbon steels "A" & "B" simulated in chloride solution

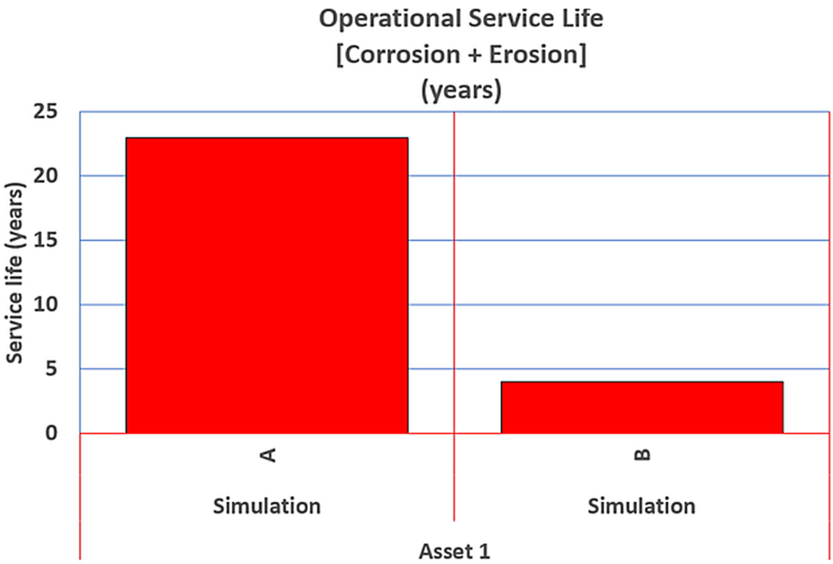


Figure 35. AssessLIFE software result: simulated degradation driver contribution (mm/yr) of carbon steels "A" & "B" in chloride solution

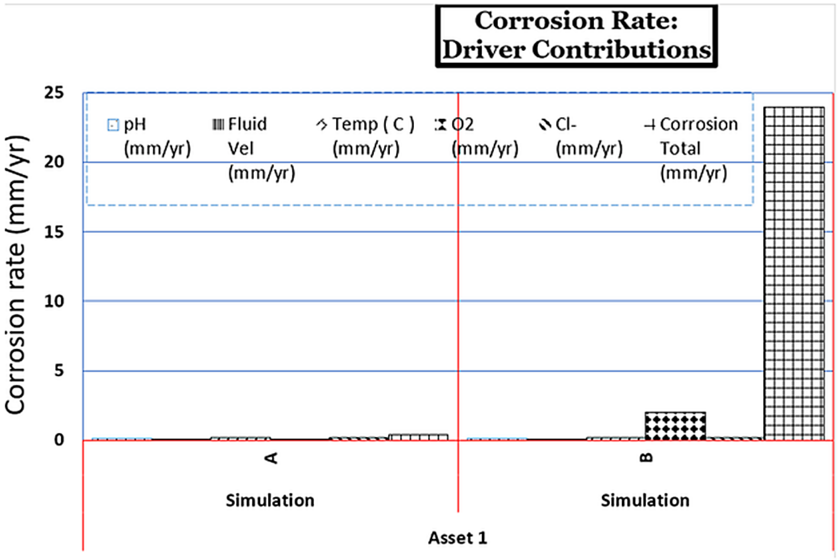
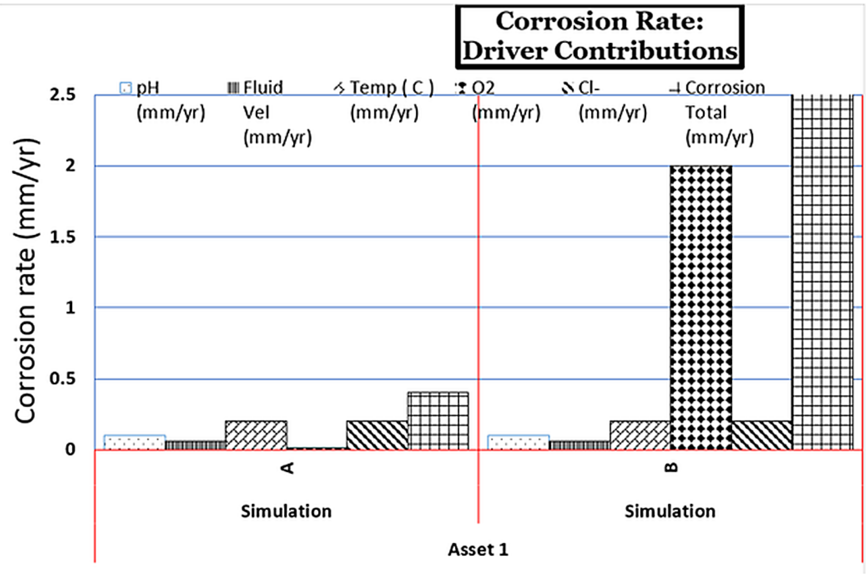


Figure 36. Rescaled version of Figure 35



(Mobin & Shabnam, 2011). Therefore, by employing tested and proven scientific analytical computations, forecasting, prediction, and analytics, the AssessLIFE software possess the capabilities to significantly reduce the billions of dollars expended in assets which degrade prematurely, enhance personal and asset safety, and generate financial benefits for its users.

AssessLIFE Software: The Effect of Flow Velocity on the Pitting Corrosion of 316l Stainless Steels in Chloride Solution

Table 2 shows the exposure parameters of two identical 316L stainless steel alloys in a saturated chloride solution. The exposure parameters for the two alloys are identical – except for the flow velocity on alloy “A” which is 0.5 m/s in contrast to the 2.0 m/s flow velocity on alloy “B”. The AssessLIFE software user inputs these parameters into the software user interface and simulates the pitting corrosion attack via the “wet corrosion” degradation mechanism. Figure 37 shows that by increasing the flow velocity on the alloys from 0.5 m/s to 2 m/s, the lifespan of the 316L alloy increased from 2 to 26 years. It is postulated that the increased flow velocity increased flow turbulence at the alloy-fluid interface. Greater flow turbulence acts to scour the surface of the alloy and disrupts the embedment of chloride into the alloy which typically progresses pitting corrosion attack. Similar results were obtained by Wharton et al who investigated the influence of flow conditions on

Figure 37. AssessLIFE software result: simulated degradation driver contribution (mm/yr) of Stainless steels "A" & "B" in chloride solution

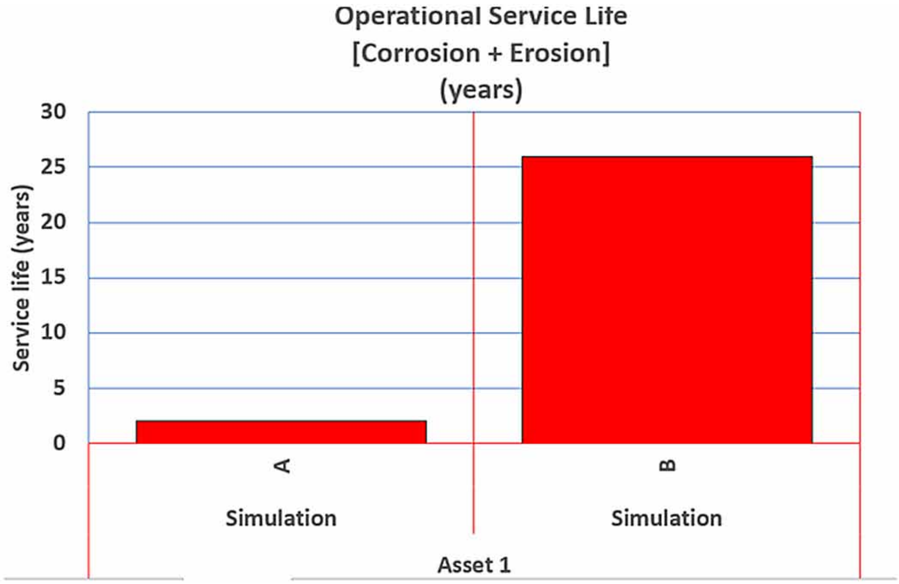


Table 2. Parameters for stainless steel corrosion simulation

316L Stainless Steel Alloy	Oxygen (ppb)	Temperature (C)	pH	Flow Velocity (m/s)	Chloride Conc (wt %)	Thickness (mm)
A	15000	50	8	0.5	20	3.4
B	15000	50	8	2.0	20	3.4

the corrosion of AISI 304L stainless steel in chloride media (Wharton & Wood, 2004). The authors noted that "stable pitting was most evident during the laminar flow regime immediately before the transition [to turbulent to flow] and near the critical velocity of (~ 1.5 ms^{-1}). Above the critical velocity the viscous sublayer can be considered thin enough for high-speed fluid (sweep events) to penetrate across it, to the metal surface, with sufficient kinetic energy to disturb the growth of metastale pitting, thus impeding the growth of stable pits".

CONCLUSION

This paper has proposed an AssessLIFE software to address the strategic deficiency arising from the continuous degradation of metallic industrial assets, equipment and components which often result in crumbling infrastructure, and thus requiring industries to expend billions of dollars on mitigation strategies. The proposed software has the potential to enhance personnel safety in physical asset management by generating diagnosis and analytics on asset lifespan and health status. Alloy degradation costs the global economy billions of dollars a year. By employing tested and proven scientific analytical computations, forecasting, prediction, and analytics, AssessLIFE software plans to significantly reduce the billions of dollars wasted as cost of alloy degradation as well as reduce the billions of dollars expended via inspection, treatment, and repair of degradation-prone assets and infrastructure. AssessLIFE software estimates asset lifespan and other analytics via mathematical modeling, integration, and automation, and then provides various industry stakeholders with useful information to make better decisions in areas of industrial asset management.

REFERENCES

ASTM International. (2003). ASTM G48-03 Standard Test Methods for Pitting and Crevice Corrosion Resistance of Stainless Steels and Related Alloys by Use of Ferric Chlorde Solution. *ASTM G48-03*, 1-11.

Badr, H. M., Habib, M. A., Ben-Mansour, R., & Said, S. (2005). Numerical Investigation of Erosion Threshold Velocity in a Pipe With Sudden Contraction. *Computers & Fluids*, *34*(6), 721–742. doi:10.1016/j.compfluid.2004.05.010

Bahadori, A. (2015). *Essentials of Coating, Painting, and Lining for the Oil, Gas, and Petrochemical Industries*. Elsevier Inc.

Blume, S. W. (2007). *Electrical Power Systems Basics: For the Nonelectrical Professional*. John Wiley & Sons. doi:10.1002/9780470185810

Bui, A., Johnson, F., & Wasko, C. (2019). The Relationship of Atmospheric Air Temperature and Dew Point Temperature to Extreme Rainfall. *Environmental Research Letters*, *14*(7), 1–8. doi:10.1088/1748-9326/ab2a26

Casesnoves, F., & Surzhenkov, A. (2017). A Mathematical Model For Abrasive Erosion Wear In Composite Fe-Based Matrix With WC-CO Reinforcement. *WIT Transactions on Engineering Sciences*, *116*, 99–111. doi:10.2495/MC170101

Choudary, R. B. (2003). *Materials Science & Metallurgy* (1st ed.). Khanna Publishers.

Cicek, V. (2013). *Cathodic Protection: Industrial Solutions For Protecting Against Corrosion*. Scrivener Publishing LLC. doi:10.1002/9781118737880

Do, K. H., & Roy, S. K. (1994). Corrosion of steel in tropical sea water. *British Corrosion Journal*, *29*(3), 233–236. doi:10.1179/000705994798267665

Dupont, J. N., Lippold, J. C., & Kiser, S. D. (2009). *Welding Metallurgy and Weldability of Nickel-Base Alloys*. John Wiley & Sons. doi:10.1002/9780470500262

Ebeling, C. E. (1997). *An Introduction To Reliability and Maintainability Engineering*. The McGraw-Hill Companies.

Edeleanu, C. (1960). Corrosion Control By Anodic Protection. *Platinum Metals Review*, *4*(3), 86–91.

Edited by Boyer Howard E. (2020). *Ninth Printing). Atlas of Fatigue Curves*. ASM International.

Elfergani, H. A., & Abdalla, A. A. (2017). Effect of Chloride Concentration on the Corrosion Rate of Carbon Steel. In *2nd Libyan Conference On Chemistry and Its Application (LCCA)* (pp. 33-38). Benghazi: Libyan Conference on Chemistry and Its Application.

Elsevier. (1991). Fundamentals of Fluid Dynamics. *International Geophysics, 47*, 7-83. doi:10.1016/S0074-6142(09)60056-5

Ertas, A. (2012). *Engineering Mechanics and Design Applications: Transdisciplinary Engineering Fundamentals*. Taylor & Francis Group, LLC.

Frenzel, L. E. Jr. (2018). *Electronic Explained: Fundamentals for Engineers, Technicians, and Makers* (2nd ed.). Elsevier Inc.

Ghasem, N., & Henda, R. (2009). *Principles of Chemical Engineering Processes*. Taylor & Francis Group, LLC.

Glastone, S., & Mehra, V. (2011). Practical Fundamentals of Chemical Engineering (8th ed.). IDC Technologies.

Haanappel, V. A., & Stroosnijder, M. F. (2001). Influence of Mechanical Deformation on the Corrosion Behavior of AISI 304 Stainless Steel Obtained from Cooking Utensils. *Corrosion*, *57*(6), 557–565. doi:10.5006/1.3290382

Hipple, J. (2017). *Chemical Engineering for Non-Chemical Engineers*. American Institue of Chemical Engineers. doi:10.1002/9781119369196

Hutchings, I. (1992). Abrasive and Erosive Wear of Metal-Matrix Composites. In *2nd European Conference on Advanced Materials and Processes*. London: Institute of Materials.

Jones, D. A. (1996). *Principles and Prevention of Corrosion* (2nd ed.). Prentice-Hall, Inc.

Kececi, E. F. (2019). *Mechatronic Components: Roadmap to Design*. Elsevier Inc.

Kosa, E., & Goksenli, A. (2017). Influence of Material Hardness and Particle Velocity On Erosive Wear Rate. *Jixie Gongcheng Xuebao*, *47*, 8–14.

Kotecki, D. J., & Lippold, J. C. (2005). *Welding Metallurgy and Weldability of Stainless Steels*. John Wiley & Sons Inc.

Levy, A. V. (1995). *Solid Particle Erosion and Erosion-Corrosion of Materials*. ASM International.

Levy, A. V., & Chik, P. (1983). The Effects of Erodent Composition and Shape on the Erosion of Steel. *Wear*, *89*(2), 151–162. doi:10.1016/0043-1648(83)90240-5

Lippold, J. C. (2015). *Welding Metallurgy and Weldability*. John Wiley & Sons, Inc. doi:10.1002/9781118960332

Mobin, M., & Shabnam, H. (2011). Corrosion Behavior of Mild Steel and SS 304L in Presence of Dissolved Nickel Under Aerated and DeAerated Conditions. *Materials Research*, *14*(4), 524–531. doi:10.1590/S1516-14392011005000076

Obi, E. R. (2008). *Corrosion Behaviour of Fly Ash-Reinforced Aluminum-Magnesium Alloy A535 Composites*. University of Saskatchewan, Mechanical Engineering. Retrieved from https://harvest.usask.ca/handle/10388/etd-09222008-235440

Okonkwo, P. C. (2014). Erosion-Corrosion in Oil and Gas Industry: A Review. *International Journal Of Metallurgical & Material*, *4*(3), 7–28.

Phillips, D. H. (2016). *Welding Engineering: An Introduction*. John Wiley & Sons Ltd. doi:10.1002/9781119191407

Pourbaix, M. (1974). *Atlas of Electrochemical Equilibria in Aqueous Solutions*. National Association of Corrosion Engineers.

Rauf, S. B. (2014). *Electrical Engineeering for Non-Electrical Engineers*. The Fairmont Press, Inc.

Revie, R. W., & Uhlig, H. H. (2008). *Corrosion and Corrosion Control: An Introduction to Corrosion Science and Engineering*. Wiley-InterScience. doi:10.1002/9780470277270

Schweitzer, P. A. (2006). *Paint and Coatings: Applications and Corrosion Resistance*. Taylor & Francis Group, LLC.

Sedriks, J. A. (1996). *Corrosion of Stainless Steels*. John Wiley & Sons, Inc.

Shehadeh, M., Anany, M., Saqr, K. M., & Hassan, I. (2014). Experimental Investigatio of Erosion-Corrosion Phenomena in a Steel Fitting Due to Plain and Slurry Seawater Flow. *International Journal of Mechanical and Materials Engineering*, *9*(22), 1–8.

Simillion, H., Dolgikh, O., Terryn, H., & Deconinck, J. (2014). Atmospheric corrosion: A review focussed on modelling. *Corrosion Reviews*, 1–42.

Singh, R. (2012). *Applied Welding Engineering: Processes, Codes And Standards*. Elsevier Inc.

Soares, G., Garbatov, Y., & Zayed, A. (2011). Effect of Environmental Factors on Steel Plae Corrosion under marine Immersion Conditions. *Corrosion Engineering, Science and Technology*, *46*(4), 524–541. doi:10.1179/147842209X12559428167841

Stack, M. M., Chacon-Nava, J., & Stott, F. H. (1995). Relationship Between the Effects of Velocity and Alloy Corrosion Resistance in Erosion-Corrosion Environment at Elevate Temperatures. *Wear*, *180*(1-2), 91–99. doi:10.1016/0043-1648(94)06536-5

Subir, P. (2010). Estimation of Corrosion Rate of Mild Steel in Sea Water and Application of Genetic Algorithms to Find Minimum Corrosion Rate. *Canadian Metallurgical Quarterly*, *41*(1), 1–8.

Taghavi-Zenouz, R., Salari, M., & Etemadi, M. (2008). Prediction of Laminar, Transitional and Turbulent Flow Regimes Based on Three Equation k-w Turbulence Flow. *Aeronautical Journal*, *112*(1134), 469–476. doi:10.1017/S0001924000002438

The Materials Information Society. (2006). *Corrosion of Weldments* (J. R. Davis, Ed.). ASM International.

Turian, R. M., Hsu, F. L., & Ma, T. W. (1987). Estimation of the Critical Velocity in Pipeline Flow of Slurry. *Powder Technology*, *51*(1), 35–47. doi:10.1016/0032-5910(87)80038-4

Ukhurebor, K., Batubo, T., Abiodun, I., & Enoyoze, E. (2017). The Influence of Air Temperature on the Dew Point Temperature in Benin City, Nigeria. *Journal of Applied Science & Environmental Management*, *21*(4), 657–660. doi:10.4314/jasem.v21i4.5

Wada, S., & Watanalm, W. (1987). *Solid gerlicle erosion in ~itte materials Part 3. The intersection with hi.ella[pl~pertles of target and th~z of impinginement particles on erosion wear mechanism*. Yogyo-Kyokai shL.

Wharton, J. A., & Wood, R. K. (2004). Influence of Flow Conditions on the Corrosion of AISI 304L Stainless Steel. *Wear*, *256*, 525–536.

Winkelaar, A. (2009). *Coating Basics*. Vincentz Network, GmbH & Co. KG.

Zelinka, S. L., Glass, S. V., & Derome, D. (2014). The Effect of Moisture Content on the Corroson of Fasteners Embedded in Wood Subjected to Alkaline Copper Quaternary Treatment. *Corrosion Science*, *83*, 67–74. doi:10.1016/j.corsci.2014.01.044

Chapter 3
A Network Data Analytic Technique in a 5G-IoT-Based Smart Healthcare System Using Machine Learning

Neha Gupta
Graphic Era University (Deemed), India

Pradeep Juneja
Graphic Era University (Deemed), India

Sachin Sharma
Graphic Era University (Deemed), India

Umang Garg
Graphic Era Hill University, India

ABSTRACT

Healthcare is an important part of every individual's life. Unfortunately, the rising prevalence of chronic diseases is putting a burden on the modern healthcare system. The internet of things (IoT) with 5G technology offers a number of advantages to the healthcare system, including remote monitoring, remote robotic surgery, and ambulances operating on dedicated network slices, all of which relieve pressure on the traditional healthcare system. 5G-IoT enables billions of healthcare equipment to communicate with one another. These devices will produce a huge amount of data that can be evaluated. In the healthcare industry, data analytics has a huge potential. In this chapter, the authors examine a brief history of machine learning as well as some fundamental knowledge of the methodologies. In addition, the author has provided a brief overview of several machine learning algorithms utilized in healthcare in the context of 5G-IoT. The future aspect of machine learning in a 5G-IoT smart healthcare system was also highlighted.

DOI: 10.4018/978-1-6684-3855-8.ch003

INTRODUCTION

The healthcare industry is constantly changing and offers numerous research opportunities. The healthcare system is referred to as a smart system due to the rapid expansion and advancement of technology such as 5G, IoT, machine learning, and artificial intelligence (Islam et al., 2020). Several modern medical gadgets and sensors can communicate over multiple networks via IoT, providing access to critical information regarding a patient's condition. This information can subsequently be used for a variety of purposes, including remote patient monitoring, bettering the diagnosis and treatment process through improved automation and mobility, and anticipating disease and recovery through a deeper understanding of symptoms (Ahad et al., 2019).

The presentation of 5G innovation fundamentally affects the medical services area. There is a portion of the critical highlights of 5G correspondence like fast information transmission, enormous inclusion region, control network traffic with a high limit, profoundly responsive, minimal expense. Likewise, the capacity to interface much more gadgets on the double (for sensors and brilliant wise intuitive gadgets) is one of the significant key highlights of 5G correspondence modules to work on tolerant involvement in customized, protection care. Consolidating a fast 5G cell network into brilliant medical care can support the trustworthy and quick transmission of huge clinical imaging documents with information sizes of approximately 1 gigabyte for each quiet review (Brito, 2018). One of the predominant uses of 5G in medical care is mHealth. mHealth represents versatile wellbeing. It has alluded to the blend of portable correspondences, wearable detecting, and clinical innovations for advantageous and distant medical care conveyance (Thayananthan, 2019).

ML calculations have shown to be profoundly valuable in medical care because of the gigantic measure of information gathered continuously by 5G empowered IoT gadgets and their intricacy. These calculations empower us to separate significant realities from the information we've assembled and settle on choices dependent on it. The utilization of ML-based frameworks has various benefits. They can be prepared to utilize enormous volumes of information, alluded to as preparing information, and afterward utilized in clinical practice to help with hazard appraisal and treatment plan through inductive deduction. Accordingly, AI calculations work on the productivity of the framework. Computerized reasoning (AI) can assist doctors with counselling and give the best understanding consideration by concentrating on clinical science information from course books, diaries, and clinical practices, which is tedious for people (Najm et al., 2019). Existing AI draws near, then again, can't arrive at similar decisions as a human brain. Observing, making do, and investigating clinical data becomes more straightforward with the reconciliation of AI with 5G-IoT gadgets in medical care. Existing AI draws near, then again, does not have the determinations that a human psyche can reach. Checking, making do, and breaking down clinical data becomes more straightforward with the reconciliation of AI with 5G-IoT gadgets in medical services.

Although there has been a ton of work done in the space of 5G, IoT, and AI in medical services, its vast majority has been centered around the design rather than the variety of calculations or how the information is showing up from 5G-IoT gadgets. Therefore, we endeavoured to overcome any issues by investigating a few designs for both IoT frameworks and ML models. Coming up next are the essential commitments of this work.

1. An outline of different noticeable ML calculations with a specific spotlight on their applications and use cases in 5G empowered IoT medical care industry has been given.
2. Futuristic effect of AI in the 5G Enabled IoT medical care has been considered.

The remainder of the paper is coordinated in an accompanying way: area II gives the connected work in the field of 5G, IoT, AI in medical care. Segment III gives a short outline of the different ML calculations as of now being explored for utilization in the medical services industry. Segment IV gives the future part of AI in 5G empowered savvy medical services framework. At long last, segment V gives the end to the paper.

RELATED WORK

In this part, we present a rundown of some distributed past businesses related to the utilization of AI in medical services, 5G, and IoT. The part likewise remembers some current work for zeroed in on 5G-IoT in medical services.

Ihab Ahmed Najm et al (Najm et al., 2019) proposed another AI model dependent on a choice tree (DT) calculation to anticipate the ideal upgrade of blockage control in the remote sensors of 5G IoT organizations. The model was carried out on a preparation dataset to decide the ideal parametric setting in a 5G climate. The dataset was utilized to prepare the AI model and empower the expectation of ideal options that can upgrade the exhibition of the blockage control approach. Amine Rghioui et al (Rghioui et al., 2020) present an astute design for observing diabetic patients by utilizing AI calculations. The design components included shrewd gadgets, sensors, and cell phones to gather estimations from the body. The astute framework gathered the information got from the patient and performed information grouping utilizing AI to make an analysis. A few AI calculations were utilized to assess the proposed forecast framework. Jaime Lloret et al. (Lloret et al., 2017) describe a design for astute eHealth monitoring of recurrent patients. Wearable gadgets are used to collect measurements from the body, and a mobile phone is used by the patient to manage the data collected by the wearable gadgets. The intelligent framework analyses and generates alerts using AI in BigData from various medical clinics and patient information.

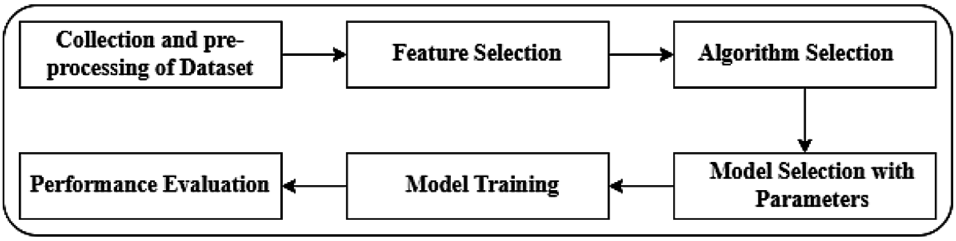
Anusorn Charleonnan et al (Charleonnan et al., 2017) offer AI algorithms for predicting chronic renal disease based on clinical data. K-closest neighbours (KNN), support vector machine (SVM), strategic relapse (LR), and decision tree classifiers are among the AI techniques researched. These predictive models were created using a dataset of ongoing kidney disease, and the results of these models were compared to find the best classifier for predicting chronic kidney disease. Zixian Wang et al (Wang et al., 2018) has examined different AI procedures, especially characterization and affiliation methods, to foresee CKD and broke down the impacts of involving highlight choice strategies in mix with grouping methods. The CKD dataset is benchmarked using WEKA-based characterization methods. The results are calculated using a 10-overlay cross-approval method with and without the component selection technique. Hyun Yoo et al. (Yoo et al., 2020) present a model for customized heart condition characterization in combination with a quick and compelling pre-handling method and deep neural organization to deal with continuous aggregated biosensor input information, which can be useful for learning input information and fostering an estimated work, as well as assisting clients in perceiving hazard situations.

Kanchan Pradhan et al (Pradhan & Chawla, 2020), investigated 65 changed papers for foreseeing various sicknesses, utilizing AI calculations. The investigation principally centers around different AI calculations utilized for recognizing a few sicknesses to look for a hole toward the future improvement for distinguishing cellular breakdown in the lungs in clinical IoT. Arun Kumar et al. (Kumar et al., 2021) focused on the execution of innovative waveforms such as non-symmetrical various access (NOMA), Universal channel multi-transporter (UFMC), and channel bank multi-transporter (FBMC). A few boundaries of cutting-edge waveforms and OFDM techniques are explored and considered, such as power range thickness, bit error rate, limit, and PAPR. Xiaochun Cheng et al (Cheng et al., 2021) provide a summary of the articles, which are late advancements in the 5G-IoT sector. Farhan Ullah et al (Ullah et al., 2021) developed a hybrid approach to dealing with the Control Flow Graph (CFG) and a deep learning model to provide smart 5G-IoT administrations.

MACHINE LEARNING ALGORITHMS

AI (ML) is a class of computerized reasoning that empowers PCs to think and learn all alone. Everything revolves around persuading PCs to change their movement in order to work on the activities with greater precision, where precision is measured in terms of the number of times the chosen activities result in the correct ones (Alzubi et al., 2018). AI is a multi-disciplinary field having a wide scope of examination spaces supporting its reality. The nonexclusive model of AI comprises six parts autonomous of the calculation taken on as displayed in fig 1.

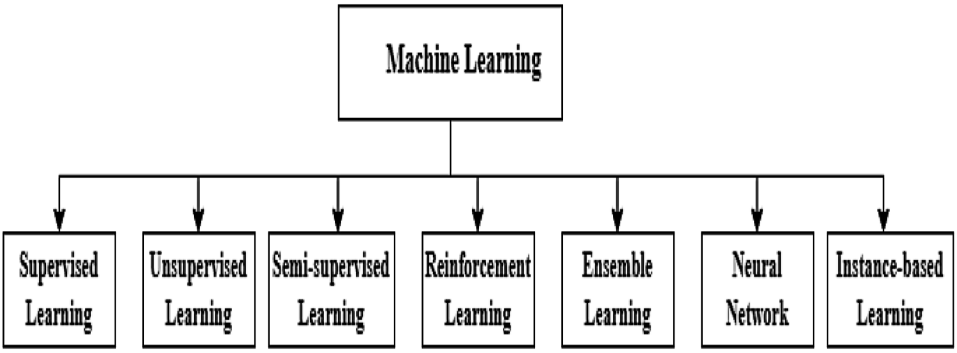
Figure 1. Components of a generic ML model



It is necessary to train PCs to competently carry out the task without human intervention, based on learning and continually expanding experience, in order to appreciate the issue's complexity and the need for flexibility. AI has demonstrated capacities to innately take care of the issues of information science. Information science is characterized as, "an idea to bring together measurements, information investigation, AI and their connected techniques to comprehend and examine real peculiarities" with information". Any issue in information science can be assembled in one of the accompanying five classes.

The medical services space has an immense measure of information, so AI is a scientific apparatus to tackle the information-related issues in the medical services area. It depends on the various calculations to tackle information issues. The sort of calculation utilized relies upon the sort of issue we wish to tackle, the quantity of factors, the sort of model that would suit it best, etc (Batta, 2020). Here is a glance in fig 2. at a portion of the regularly involved calculations in AI.

Figure 2. Different machine learning algorithm



Machine learning algorithm: In this segment, we centre around some famous AI calculations. These calculations have a wide area of common-sense applications, some of the calculations are depicted exhaustively in Table 1.

Table 1. Literature review of past work done

Paradigm	Algorithm	Description
Supervised Learning	Decision Tree	The learning capacity is addressed as a choice tree in the Decision Tree approach for approximating discrete esteemed objective capacities. A choice tree isolates occurrences dependent on highlight esteems by requesting them from root to leaf hubs. Each branch is a potential incentive for that element, and every hub addresses a choice (test condition) on a quality of the case. The root hub for an occasion's characterization is the choice hub. The tree falls along the edge that compares to the hub esteem that relates to the worth of the component test result (Kullarni & Sinha, 2013). This procedure is rehashed in the sub-tree lead by the new hub at the edge's end. At last, the arrangement classes or extreme judgment are addressed by the leaf hub. The motivation behind a choice tree is to figure out which property at every hub level is the best classifier. Factual measurements, for example, data gain, Gini file, Chi-square, and entropy are determined to decide the worth of every hub. An assortment of calculations is utilized to carry out choice trees. Among the most well-known are Classification and Regression Tree (CART), Iterative Dichotomiser 3 (ID3), Automatic Interaction Detection (CHAID), Chi-Squared C4.5, and C5.0, and M5.

Continued on following page

Table 1. Continued

Paradigm	Algorithm	Description
	Naïve Bayes	Naive Bayes uses Bayes' Theorem of Probability to categorize. The posterior probability of an event (A) given a prior probability of event B (P(A/B)) is calculated using Bayes' theorem as follows: P(B/A) = P(A/B) P(A) P(B) ● There are two events: A and B. ● The probabilities of seeing A and B independently are P(A) and P(B). ● The conditional probability, or the possibility of seeing A if B is true, is P(A/B). ● If A is True, P(B/A) is the probability of witnessing B. Basic probabilistic classifiers dependent on the Bayes' Theorem with solid freedom limitations among the traits are known as guileless Bayes' classifiers (Bhardwaj et al., 2017). It's very beneficial when the inputs have a lot of dimensions.
	Support Vector Machines	SVMs are helpful for both arrangement and relapse. It's a learning calculation that is regulated. It depends on the idea of ascertaining edges. Every information thing is plotted as a point in n-layered space (where n is the quantity of highlights in our dataset) utilizing this procedure (Alzubi et al., 2018). Each component's worth is the matching direction's worth. It isolates the information into classes by choosing a line (hyperplane) that separates the preparation datasets into gatherings. It works by expanding the cradle between the closest item (in the two classes) and the hyperplane (Evgeniou & Pontil, 2001).
	Regression Analysis	Regression examination is a sort of prescient displaying to research the connection between at least one autonomous factor and a reliant variable. It's an unquestionable requirement to have program for information examination and display. By fitting the line/bend to the relevant elements, this technique attempts to decrease variations in information point good ways from the bend or line. Relapse examination is partitioned into three sorts: direct, calculated, and polynomial (Li & Wu, 2012).
Unsupervised Learning	K-Means Clustering	For group investigation, K-implies is a famous solo AI procedure. Its motivation is to separate a bunch of 'n' perceptions into a bunch of 'k' groups, with every perception having a place with the bunch with the nearest mean, which fills in as the bunch's model. The group's middle is characterized by the mean of the perceptions in the bunch (Li & Wu, 2012).
Instance based Learning	K-nearest Neighbours	It is a non-parametric order and relapse strategy. The KNN method finds the k-closest neighbors of an obscure element vector whose class should be distinguished utilizing N preparing vectors (Taunk, 2019).

Continued on following page

Table 1. Continued

Paradigm	Algorithm	Description
Ensemble Learning	Random Forest	It's a characterization and relapse calculation dependent on group learning. It assembles a whirlwind of choice trees from an arbitrary cut of information utilizing a sacking calculation. Random trees are framed by consolidating the aftereffects of all choice trees in the arbitrary woodland. The Random Forest Algorithm has two phases: the first is to make irregular woods, and the second is to foresee utilizing the arbitrary backwoods classifier set up in the principal stage (Kullarni & Sinha, 2013).
Dimensionality Reduction	Principal Component Algorithm	It is much of the time used to decrease the quantity of aspects in an informational index. It supports decreasing both the quantity of information assortment highlights and the quantity of autonomous factors. It utilizes symmetrical change to change associated information into a bunch of straightly uncorrelated factors alluded to as guideline parts (Najm et al., 2019).

Sources: Research conducted by researchers

1. **Applications of machine learning in 5G-IoT based healthcare system:** Because of the developing number of AI applications in medical care, we can picture a future where information, investigation, and advancement cooperate to help incalculable individuals without stressing over determination, identification, or anticipating. A huge infrastructure of medical devices currently generates data, but there is frequently no supporting infrastructure in place to efficiently exploit that data (Mustafa & Rahimi Azghadi, 2021). Medical data is available in a number of forms, which can make data preparation more difficult and increase noise. Here are some examples of possible application areas:
    a. **Disease Recognition and Diagnosis:** One of the main utilization of AI in medical services is the discovery and conclusion of illnesses and sicknesses that are generally hard to analyze. This can incorporate anything from malignant growths that are hard to recognize right off the bat to other acquired illnesses.
    b. **Drug Development and Production:** In the beginning phases of medication research, one of the most widely recognized clinical utilization of AI is in drug improvement. This incorporates innovative work instruments like cutting edge sequencing and accuracy medication, which can assist with tracking down original medicines for troublesome sicknesses Unaided learning is currently utilized in AI calculations to reveal designs in information without producing forecasts (Lloret et al., 2017).

c. **Diagnosis based on medical imaging:** Combining AI and profound learning have brought about the inventive methodology known as Computer Vision. Microsoft's Inner Eye drive, which centers around picture indicative instruments for picture examination, has supported this. As AI turns out to be more open and their informative limit created, hope to see more information sources from different clinical imaging turning into a piece of this AI-driven conclusion process (Mustafa & Rahimi Azghadi, 2021).

d. **Individualized Medicine:** Personalized medicines can in addition to the fact that more be fruitful when individual wellbeing and prescient investigation are joined, yet they are additionally ready for more examination and better infection assessment. Doctors are at present restricted to look over a rundown of findings or evaluating a patient's danger dependent on his clinical history and promptly accessible hereditary information.

e. **Behavioral modification based on machine learning:** Behavioral adjustment is a significant piece of preventive medication, and since the ascent of AI in medical care, a harvest of new organizations have sprung up in the space of disease anticipation and finding, patient therapy, etc.

f. **Smart Health Records:** Keeping current wellbeing records is a tedious action, and keeping in mind that innovation has helped the information section process, a large portion of the exercises actually consume most of the day to achieve (Kumar et al., 2021). The key job of AI in medical services is to smooth out methodology to save time, exertion, and cash. Two instances of record arrangement frameworks that utilization vector machines and ML-based OCR acknowledgment procedures that are consistently acquiring consideration are Google's Cloud Vision API and MATLAB's AI based penmanship acknowledgment innovation.

g. **Clinical Research and Trials:** Machine learning offers an assortment of utilizations in clinical preliminaries and exploration. Clinical preliminaries, as anyone in the drug business knows, take a ton of time and cash to finish and can require a very long time in specific cases. Specialists can set up a pool of potential clinical preliminary candidates utilizing AI based prescient investigation from an assortment of information sources, including past specialist visits, online media, and more.

h. **Improved Radiotherapy:** One of the most pursued employments of AI in medical care is in the area of radiology. In clinical picture examination, there are different discrete factors that can change whenever. Utilizing progressed conditions, numerous injuries, disease foci, and different occasions are trying to demonstrate. Diagnosing and observing factors gets more straightforward with ML-based calculations since they gain from an enormous number of various examples. One of the most unmistakable employments of AI in clinical picture examination is the arrangement of items into classifications like ordinary or unusual, sore or non-injury, etc.

2. **Future aspect of Machine learning in 5G-IoT smart healthcare system:** Medical care is a huge industry that conveys superior grade, financially savvy care to a huge number of individuals while likewise procuring significant income for some states. In the present market, the medical services industry in the United States creates $1.668 trillion in income. Besides, the United States spends more on medical care per capita than most of other industrialized and helpless nations. In the medical care market, quality, worth, and result are three popular expressions that guarantee a great deal (Thayananthan, 2019). One of the main pieces of medical services is fast navigation. AI for medical services progresses consistently. It can manage vast amounts of data and deliver important insights to help healthcare practitioners make timely decisions. People desire improved health results, while doctors want to cut down on the amount of time and money they spend on each patient. In the operating area, robots might be programmed to aid surgeons. Machine learning can help surgeons reduce risk during surgeries by focusing on the smallest components of the operations (Mustafa & Rahimi Azghadi, 2021). In the coming years, it will extend its healthcare base. As a result, machine learning will make 5G-IoT-based healthcare systems faster and more advanced in the future.

CONCLUSION

In the realm of healthcare, the use of digital technologies such as machine learning is entering a new phase. Machine learning is being utilised in healthcare to improve patient outcomes by utilising the growing amount of health data provided by 5G-Internet of Things. Decision trees, Nave Bayes, Support vector machines, regression analysis, K-means clustering, and other machine learning algorithms are briefly reviewed in this paper and show potential in healthcare. The types of problems we want to address determine which strategies we apply. Machine learning is used in three key areas: medical imaging, natural language processing of medical records, and genetic information. Behavioural modification, smart health records, clinical trials and research, and improved radiotherapy are some of the other domains where machine learning is used effectively and covered in this study. The healthcare industry in the United States alone generates $1.668 trillion in sales. It is a business that provides millions of people with a value-based core. As a result, numerous countries, including India, are becoming the top income earners now and in the future. As a result, machine learning helps the healthcare industry progress.

REFERENCES

Ahad, A., Tahir, M., & Yau, K. L. A. (2019). 5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 100747–100762. doi:10.1109/ACCESS.2019.2930628

Alzubi, J., Nayyar, A., & Kumar, A. (2018). Machine Learning from Theory to Algorithms: An Overview. *Journal of Physics: Conference Series*, *1142*(1), 012012. Advance online publication. doi:10.1088/1742-6596/1142/1/012012

Batta, M. (2020). Machine Learning Algorithms - A Review. *International Journal of Science and Research, 9*(1). doi:10.21275/ART20203995

Bhardwaj, R., Nambiar, A. R., & Dutta, D. (2017). A Study of Machine Learning in Healthcare. *Proceedings - International Computer Software and Applications Conference, 2*, 236–241. 10.1109/COMPSAC.2017.164

Brito, J. M. C. (2018). Technological trends for 5G networks influence of E-Health and IoT applications. *International Journal of E-Health and Medical Communications*, *9*(1), 1–22. doi:10.4018/IJEHMC.2018010101

Charleonnan, A., Fufaung, T., Niyomwong, T., Chokchueypattanakit, W., Suwannawach, S., & Ninchawee, N. (2017). Predictive analytics for chronic kidney disease using machine learning techniques. *2016 Management and Innovation Technology International Conference, MITiCON 2016*, MIT80–MIT83. 10.1109/MITICON.2016.8025242

Cheng, X., Zhang, C., Qian, Y., Aloqaily, M., & Xiao, Y. (2021). Editorial: Deep learning for 5G IoT systems. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3049–3051. doi:10.100713042-021-01382-w PMID:34306244

Evgeniou, T., & Pontil, M. (2001). Support vector machines: Theory and applications. Lecture Notes in Computer Science, 2049, 249–257. doi:10.1007/3-540-44673-7_12

Islam, M. M., Rahaman, A., & Islam, M. R. (2020). Development of Smart Healthcare Monitoring System in IoT Environment. *SN Computer Science*, *1*(3), 185. Advance online publication. doi:10.100742979-020-00195-y PMID:33063046

Kullarni, V. Y., & Sinha, P. K. (2013). Random Forest Classifier: A Survey and Future Research Directions. *International Journal of Advanced Computing*, *36*(1), 1144–1156.

Kumar, A., Dhanagopal, R., Albreem, M. A., & Le, D. N. (2021). A comprehensive study on the role of advanced technologies in 5G based smart hospital. *Alexandria Engineering Journal*, *60*(6), 5527–5536. doi:10.1016/j.aej.2021.04.016

Li, Y., & Wu, H. (2012). A Clustering Method Based on K-Means Algorithm. *Physics Procedia*, *25*, 1104–1109. doi:10.1016/j.phpro.2012.03.206

Lloret, J., Parra, L., Taha, M., & Tomás, J. (2017). An architecture and protocol for smart continuous eHealth monitoring using 5G. *Computer Networks*, *129*, 340–351. doi:10.1016/j.comnet.2017.05.018

Mustafa, A., & Rahimi Azghadi, M. (2021). Automated machine learning for healthcare and clinical notes analysis. *Computers*, *10*(2), 1–31. doi:10.3390/computers10020024

Najm, I. A., Hamoud, A. K., Lloret, J., & Bosch, I. (2019). Machine learning prediction approach to enhance congestion control in 5G IoT environment. *Electronics (Switzerland)*, *8*(6), 607. Advance online publication. doi:10.3390/electronics8060607

Pradhan, K., & Chawla, P. (2020). Medical Internet of things using machine learning algorithms for lung cancer detection. *Journal of Management Analytics*, *7*(4), 591–623. doi:10.1080/23270012.2020.1811789

Rghioui, A., Lloret, J., Sendra, S., & Oumnad, A. (2020). A Smart Architecture for Diabetic Patient Monitoring Using Machine Learning Algorithms. *Health Care*, *8*(3), 348. doi:10.3390/healthcare8030348 PMID:32961757

Taunk, K. (2019). Article. *2019 International Conference on Intelligent Computing and Control Systems, ICCS 2019, Iciccs*, 1255–1260.

Thayananthan, V. (2019). Healthcare management using ICT and IoT based 5G. *International Journal of Advanced Computer Science and Applications*, *10*(4), 305–312. doi:10.14569/IJACSA.2019.0100437

Ullah, F., Naeem, M. R., Mostarda, L., & Shah, S. A. (2021). Clone detection in 5G-enabled social IoT system using graph semantics and deep learning model. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3115–3127. Advance online publication. doi:10.100713042-020-01246-9

Wang, Z., Won Chung, J., Jiang, X., Cui, Y., Wang, M., & Zheng, A. (2018). Machine Learning-Based Prediction System For Chronic Kidney Disease Using Associative Classification Technique. *International Journal of Engineering & Technology,* *7*(4.36), 1161. doi:10.14419/ijet.v7i4.36.25377

Yoo, H., Han, S., & Chung, K. (2020). A frequency pattern mining model based on deep neural network for real-time classification of heart conditions. *Healthcare (Switzerland)*, *8*(3), 234. Advance online publication. doi:10.3390/healthcare8030234 PMID:32722657

Chapter 4
Protection of Critical Infrastructure Using an Integrated Cybersecurity Risk Management (i-CSRM) Framework

Halima Ibrahim Kure
University of Central Lancashire, UK

Augustine O. Nwajana
https://orcid.org/0000-0001-6591-5269
University of Greenwich, UK

ABSTRACT

Risk management plays a vital role in tackling cyber threats within the cyber-physical system (CPS) for overall system resilience. It enables identifying critical assets, vulnerabilities, and threats and determining suitable proactive control measures to tackle the risks. However, due to the increased complexity of the CPS, cyber-attacks nowadays are more sophisticated and less predictable, which makes risk management task more challenging. This chapter proposes an integrated cyber security risk management (i-CSRM) framework for systematically identifying critical assets through the use of a decision support mechanism built on fuzzy set theory, predicting risk types through machine learning techniques, and assessing the effectiveness of existing controls through the use of comprehensive assessment model (CAM) parameters.

DOI: 10.4018/978-1-6684-3855-8.ch004

INTRODUCTION

The primary objective of critical infrastructure is resilience by delivering its users with uninterrupted services, thus, relying on their most valuable assets such as information and communication networks, and digital data, for its continuous services (Wu et al., 2015). These assets necessitate the attainment of reliability, stability, and performance, all of which necessarily require the tight integration ofcontrol technological systems, computing and communication (Kim & Kumar, 2013). However, the cyber-physical systems (CPS) complexity and the interdependencies among its various components (people, processes, technology, multiple distributed and independently operating systems) has made it an excellent target for cybercriminals. Such systems face different security threats, including system failures (e.g., device failure, system overload), human errors (e.g., lack of access control, medical system configuration error), supply chain failures (e.g., network provider failure, power outage) and malicious actions (e.g., malware, hijacking, cyber espionage (Jalali & Kaiser, 2018). Cyber-security threats lead to any potential risks, and risks can affect all aspects of critical infrastructure. The probability of loss (Dalziell & McManus, 2004)or an uncertain occurrence that may occur and affect the organization's accomplishment of strategic, operational, and financial objectives is referred to as risk(Jasmin Harvey & Service, 2007).

The significance of protecting the critical infrastructure is significant since it can strongly affect the international market economy and the trust foundations between people and societies. Now, more than ever, shielding and securing critical infrastructures is essential, especially in the healthcare sector. The COVID19 pandemic has stressed the healthcare sector's requirements since malicious entities aggressively exploit this emergency for their benefit. For example, there is a considerable number of registered domains on the Internet that contain terms related to keywords, such as "corona", "covid", "covid19". While many of them are legitimate and focus on the pandemic, numerous domains are used to spread malware via phishing and spam campaigns. Therefore, the presence of any successful cyber-attack on the systems causes a devastating effect on the organization's critical infrastructure, its business processes, and availability of its services, reputation and the economy at large.

On the other hand, the cyber-threat landscape is evolving rapidly because threat actors' motivation and goal, attack pattern, "tactics, techniques and procedure (TTP)", tools to breach systems are becoming increasingly sophisticated. This affects the understanding of risk, its severity, and cascading risk impact level, making risk management challenging for critical infrastructure systems (Fossi et al., 2011). According to a recent Experian report, almost half of all business organisations experience at least one security incident each yea(Experian, 2015). That is why global cybersecurity spending is continuously rising to 96 billion US dollars in 2018 (Boyson, 2014). Despite efforts to develop and defend secure systems, large organisations, particularly critical infrastructure, continue to believe their infrastructure is vulnerable. The successful execution of effective cyber-attack is growing with higher frequency and on a larger scale. Rather than worrying whether they would be targets of cyber-attacks, IT managers need to focus on understanding when a cyber-attack will occur and what the consequences would be. Since cyber-attacks might be inevitable, the problem of risk prediction becomes critical: identifying which areas of a given infrastructure are the most vulnerable allows for preventive action, focusing on effective controls, and assessing the cascading risk effect is fundamental.

Therefore, there is indeed a pressing need to gather Cyber Threat Intelligence (CTI) information such as; information about the threats likely to affect the organization's assets which include; the threat actor's behaviour, used TTP (tactics, techniques and procedure) and other relevant properties so that risk type can be predicted. The detailed research conducted by researchers on different aspects of the cyber-attack problem focuses primarily on these three topics: prevention, detection and analysis.

However, only a few works proposed models for prediction such as; (Canali et al., 2014), (Lalonde Levesque et al., 2013), (Liu et al., 2015)which allowed for the adoption of preventive actions to avoid disruption services. These papers examined the demographics of users'(Yen et al., 2014), network connectivity behaviour (Yen et al., 2014), and web browsing behaviour (Canali et al., 2014), website features (Soska & Christin, 2014), network mismanagement details (Liu et al., 2015) and historical incident reports of organizations (Veeramachaneni et al., 2016) to predict cyber incidents. Despite these contributions, no work has focused on integrating ML for predicting risk types within a risk management process.

Additionally, there is a lack of focus on determining asset criticality and evaluating the effectiveness of existing controls to improve the overall risk management process. This chapter shows that many critical infrastructures tend to retain cyber-security countermeasures and techniques which have been proved inadequate in the past, and at the same time, they resist adapting more efficiently and new technologies. In a summary, critical infrastructures need a comprehensive risk management approach that ensures that their critical assets are adequately secured, threats are correctly predicted, and controls are successfully evaluated and implemented.Our research contributes to addressing these limitations by proposing a practical i-CSRM framework for critical infrastructure.

The proposed framework defines the necessary fundamental aspects of cybersecurity risk management in critical infrastructure. It contributes to the cybersecurity and risk management knowledge domain by presenting the following; Firstly, the study incorporates several relevant CSRM concepts such as threat actor attack pattern, tactic, techniques, and procedures (TTP), controls, and assets to implement the framework. The framework and its process provide an essential set of conceptual ideas, activities, and steps used to predict risk types and achieve overall cybersecurity risk management, many of which are built based on industry standards and guidelines.

APPROACH TO FRAMEWORK DEVELOPMENT: UNIFIED APPROACH

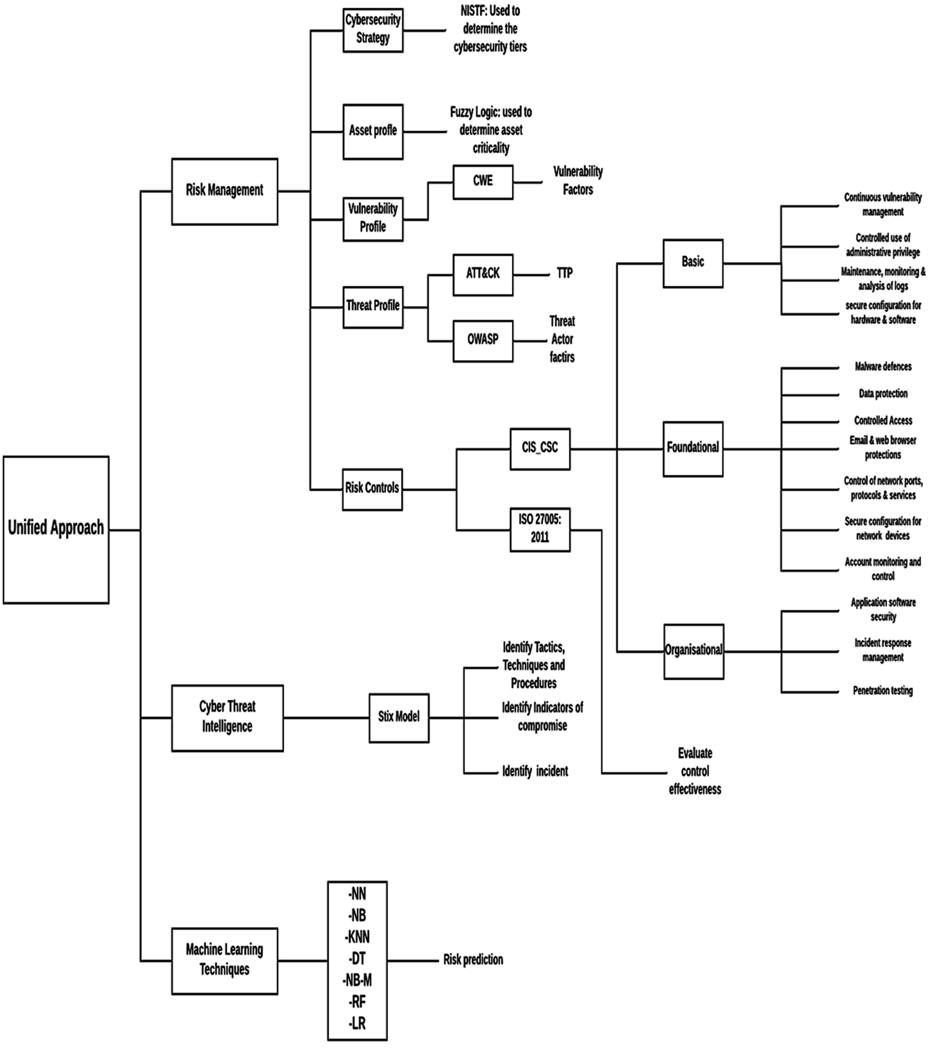
We considered four main areas for the unified approach. They include; CTI, existing risk management standards, controls and machine learning techniques. These four domains are integrated to form a unified approach used to improve risk management in critical infrastructure. Understanding threats and managing, monitoring, and communicating the presence of risks in critical infrastructure is the aim of the unified approach for the i-CSRM framework. As a result, the unified approach builds on existing industry practices to help organisations achieve overall risk control by ensuring that all steps and activities are carried out following universally agreed security criteria. For example, CIS CSC (Mbanaso et al., 2019)defines controls and assesses the efficacy of current controls using some of the parameters mentioned in (Dittmeier & Casati, 2014). The STIX model (Barnum, 2012) for identifying CTI, i.e. threat actor attack pattern and information, CWE for communicating the impacts of vulnerabilities, OWASP provides basic techniques to protect against web application security challenges, and risk management standards such as NIST SP800-30 and ISO 27005:2011 (Martin, 2007) for understanding risks in critical infrastructure. Common Attack Pattern Enumeration and Classification(CAPEC is a structured approach for understanding how an adversary operates. It provides a comprehensive list of known attacks employed by an adversary to exploit known cyber environment weaknesses. Such a model enables the identification, classification; rating, comparison and prioritisation of security risks associated with systems and applications, and this relevant model have been adopted for threat analysis for adequate cybersecurity.

The proposed approach integrates the use of fuzzy set theory for determining and ranking critical assets and integrates CSRM concepts such as threat actor, assets, TTP and controls, extracts features from these concepts so that ML classifiers can predict certain risk types. The rationale for choosing these methods is that they are widely accepted standards for raising security awareness by identifying some of the most severe cyber-physical organisations' faces.

Note that, even though the unified approach uses these approaches, our contribution is beyond these existing works and focuses on improving risk management practice using CTI information. Our approach supports analysing risks by considering the attacker's profile and the evolving threat landscape. This makes our work different from STIX, emphasising analysing the threat profile and sharing this information. On the other hand, our work integrates CTI to provide a clear and vital role in risk management by identifying, assessing, and tracking threat, as well as evaluating current vulnerabilitiesin light of such threats.Integrating CTI with CSRM helps the organisation to analyse and determine the likelihood and impact of Risk.

An overview of the different standards, frameworks, and models and the features or aspects derived from them that make it a unified approach is provided in figure 1.

Figure 1. Unified approach model


Unified Approach
Risk Management
Cybersecurity Strategy
NISTF: Used to determine the cybersecurity tiers
Asset profle
Fuzzy Logic: used to determine asset criticality
Vulnerability Profile
CWE
Vulnerability Factors
Threat Profile
ATT&CK
TTP
OWASP
Threat Actor factirs
Risk Controls
CIS_CSC
ISO 27005: 2011
Basic
Continuous vulnerability management
Controlled use of administrative privilege
Maintenance, monitoring & analysis of logs
secure configuration for hardware & software
Foundational
Malware defences
Data protection
Controlled Access
Email & web browser protections
Control of network ports, protocols & services
Secure configuration for network devices
Account monitoring and control
Organisational
Application software security
Incident response management
Penetration testing
Evaluate control effectiveness
Cyber Threat Intelligence
Stix Model
Identify Tactics, Techniques and Procedures
Identify Indicators of compromise
Identify incident
Machine Learning Techniques
-NN
-NB
-KNN
-DT
-NB-M
-RF
-LR
Risk prediction

CONCEPTUAL VIEW OF I-CSRM

The conceptual approach generally requires a straightforward understanding and precise reinterpretation of abstract ideas or principles to understand what a system, frameworks, or concepts are, what they do, how they achieve clear objectives, and how they can be implemented **(Chen, 1976).**Conceptual view accurately and precisely provides a meaning for the concepts and models the concepts such that anyone with no knowledge will understand what risk management means. It also serves as the conceptual foundation used to develop the i-CSRM framework for critical infrastructure protection.

Adopting a common terminology for the concepts would help interpret the concepts and the overall process implementation. For defining and explaining concepts in detail, conceptual modelling is highly recommended. These concepts are linked to vulnerability assessment, threat identification, risk management, and evaluating the effectiveness of existing controls. The emphasis is on the visual representation of the concepts to help their evaluation and study, utilizing logical representation for each concept.

Actor

An actor represents an individual, such as an organisation or a human user, that has a strategic goal within its organisational context and performs specific activities (Castro et al., 2002). The Actor is divided into an external and internal actor. The internal Actor is the critical infrastructure organisation that supplies infrastructure and other services needed to run its operations and has skilled personnel who play different roles such as risk manager, information technology security analyst, senior engineer. External actors are mainly users outside the organisation who make use of the services provided by the organisation. They are also third-party actors who provide various forms of computing services such as internet services and are responsible for delivering multiple other services. The listing of actors varies and will be determined in every organisation according to its volume of activities and resources. There are different types of actors, and each has a role. It consists of sub-classes such as external and internal.

Assets

Assets are necessary and have values to the organisation, such as an organisation's application or software. The critical assets are required for the stable and reliable functioning of the organisations business functions. This concept involves identifying an organisation's asset in terms of the assets used within the organisation. Assets are profiled to include categorisation according to asset criticality, asset security goal and supported business function to the organisation. The relevance of asset profiling is to help the organisation to have a standard, consistent, and clear understanding of asset boundaries, clearly designated asset goals, a description of how the asset is stored or processed, and an opportunity to determine the asset's criticality. The asset concept consists of sub-classes such as *asset types, criticality*and *asset goal, as shown in figure 3:*

- ***Asset profile:*** It describes the necessary descriptive information about the many components of all the organisation's asset types. Assets are profiled in a register to give a clear understanding of all assets and their subcomponents. The asset categories include:
  - Data are information stored and used by a computer system
  - Software is a program or application used by an organisation for its business activities. If such assets are not managed properly, they may result in financial loss, reputational damage and violation of privacy
  - Hardware is the collection of physical components of a computer system
  - Information communications and networks are the physical connection between networked computing devices using cable media or wireless media.
- ***Asset security goals:*** Each asset aims to achieve a security goal to determine the impact that may result from unauthorised access. Asset goals are established using five key areas related to information assets, including *confidentiality, integrity, Availability, accountability,* and *conformance*.
- ***Asset criticality:*** Criticality is the significant indicator used by organisations to determine which asset is of more value to the organisation. The security goals are used to measure the criticality level of each asset within the organisation. An asset type's criticality level can be from highly critical, moderately critical, to low critical. Assets are highly critical if they are the most valuable to the organisation; a moderately critical rating represents a moderate value; while low criticality means little or no value.
- ***Supported Business Process:*** business processes are structured activities or tasks backed by assets to serve a particular business objective or produce a service or product. Each asset is related to the specific business function that it supports.

Goals

The goal of any critical infrastructure includes; the concealment of sensitive data against unauthorised users, ensuring the organisation's assets are made available and accessible to the end-users, and the assets' ability to perform their required functions effectively and efficiently without any disruption or loss of service. Therefore, this concept identifies each asset's goals in terms of security and organisational context, and the security analyst carries it out. Identifying security goals is an essential consideration for an organisation to determine what fundamental security principles must be ensured for assets to be accessed or modified during storage, processing or transmission by authorised systems, applications or individuals. The assets' goals represent factors against which asset criticality is measured; they are used to distinguish those assets whose loss could significantly impact the organisation's objectives. They include:

- *Availability (A):* Availability refers to ensuring that an asset is made available and accessible to authorised users when and where they need it. This asset goal is essential, and one of the primary objectives to ensure the organisation's reliable operation. In the case the asset gets interrupted, it must be recovered and continue secure operations without noticeable effects.
- *Integrity (I):* Asset integrity refers to an asset's ability to perform its required functions effectively and efficiently without any disruption or loss of its services. The modification or destruction of an asset leads to the loss of the integrity of the asset. Loss of asset integrity may occur due to the intrusion in the cyber domain by the attacker or disgruntled employees or by human error, which degrades the asset's reliability.
- *Confidentiality (C):* Asset confidentiality refers to assets staying secured and trusted and preventing unauthorised disclosure of sensitive data. Exposure to a sensitive asset can lead to a loss of confidentiality. Confidentiality ensures that only those with predefined rights and privileges to access an asset can do so. One of the simplest methods to provide confidentiality is to install encryption/decryption components at both ends of an unsecured connection (Taylor & Sharif, 2017).
- *Accountability (ACC):* This asset goal requires that attack or incident actions that occur on an asset are tractable to the responsible system or Actor. It must be ensured that an authorised actor or an attacker who acts cannot deny involvement.
- *Conformance (CON):* This asset goal ensures that the assets such as services meet the specified standard. Assets must operate as intended without variation to expected behaviour, functions and regulatory requirements. The asset must be secured from vulnerabilities that can be exploited to cause unwanted behaviour. Any breach or deviation from specified action constitutes non-conformance.

Threat Actor

Threat actors are actors with malicious intents to execute a cyber-attack. This concept aims to allow identification and characterisation of the threat actor so that organisations can understand the attack, its trend, and the factors to determine the risk level.

TTP

This concept describes various methods in which a threat actor executes an attack and possible outcome. A threat actor uses TTP to plan and manage an attack by following a specific technique and procedure. They involve the pattern of activities or methods associated with a particular threat actor and consist of the threat actor's typical behaviour (attack pattern) and specific software tools that can be used to perform an attack. Therefore, TTP from the STIX model categorises attacks into the eleven tactics and the different techniques under each tactic provided by MITRE (Strom et al., 2017). TTP consist of sub-classes such as *initial access, execution, persistence, privileged escalation, defence evasion, credential access, discovery, lateral movement, collection, exfiltration and command and control.* These subclasses further consist of their subclasses, for example, *initial access* consists of subclasses such as *Spearphishing attachment, Spearphishing link.*

Indicator of Compromise

The indicator concept contains a pattern that can be used to detect suspicious or malicious cyber activity. IOCare detective in nature and are for specifying conditions that may exist to indicate the presence of a threat along with relevant contextual information. Organisations should be aware of the data associated with cyber-attacks, known as indicators of compromise (IOC). IOC is commonly partitioned into three distinct sub-classes (Tounsi & Rais, 2018). The sub-classes include *network indicator, host-based indicator*and *email indicator*. These sub-classes have their sub-classes, for instance, the *email indicator* has a sub-class *email attachment, email link. The network indicator* has a sub-class *IP address*.

- *Network indicators* are found in URL and domain names used for command and control and link-based malware delivery. They could be IP addresses used in detecting attacks from botnets, known compromised servers and systems conducting DDoS attack.
- *Host-based indicators* are found by analysing infected computers. They include malware names and decoy documents or file hashes of the malware

being investigated. Dynamic-link libraries (DLLs) are often targeted, and registry keys could be added by malicious code to allow for persistence.

- *Email indicators* are created when threat actors use free email services to send social engineering emails to target organisations. The email source address and subject are created from addresses that appear to be recognisable individuals or create intriguing subject lines. Attachments and links are also used for deceiving individuals.

Vulnerability

Vulnerability is the weakness or mistake in an organisation's security program, software, systems, networks, or configurations targeted and exploited by a threat actor to gain unauthorised access to an asset (system or network) using TTP. There are several ways an attacker can exploit vulnerabilities in critical infrastructures, thereby causing severe damage. This could be from a threat actor only being able to view information and to a worst-case scenario. Regardless of the Vulnerability discovered, the threat actor could have little or complete control over the system and any action taken is referred to as a cyber-attack.

Threat

The threat is the possibility of a malicious attempt to damage or disrupt an organisations asset (systems or networks), access files and infiltrate or steal data. The threat is identified as an individual or group of people attempting to gain access or exploit a vulnerability of an organisation's asset or the damage caused to hinder the organisations' ability to provide its services. Threats such as denial of service or malware attacks are famous threats to critical infrastructures, causing security challenges to the interconnected devices (Baldoni, 2014). Threat profile allows for the identification and understanding of threat characteristics. Therefore, organisations need to categorise each threat according to their goals and purpose and the assets targeted. By classifying these threats, the stakeholders check the category that a threat falls under and the most common assets affected by a particular threat. With this, a solid foundation of threat information sources is made available.

Risk

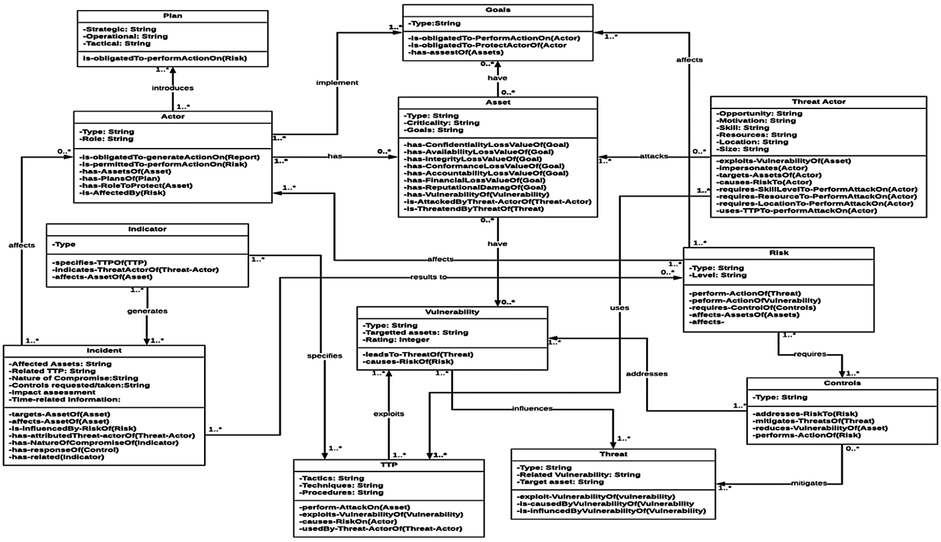
Risk is defined as the probable failure of an actor (organisation or individual) to fulfil its goals, such as confidentiality, due to the probability of a threat actor obstructing the Actor's goal. Organisations cannot wholly avoid Risk; however, it is the actors' role to ensure that risks are kept to a minimum level to achieve their goals. Therefore, organisations need to identify security risks that need to be rated. The consequence of Risk resulting from cyber-attack can lead to financial loss, reputational damage, privacy violation and non-compliance consequences, leaving users distrustful of services. To understand a cyber-attack, we have to study the nature of the attack and its motivation (Gandhi et al., 2011). Therefore, for risk severity to be estimated, it is essential for information about the threat actor, vulnerability factors and the impact of a successful exploit affecting the security goals of the assets to be gathered. The following sub-classes are involved in identifying the risk level;*threat type, vulnerability type, risk type, control type*, *Security Assets goal.*

Controls

These are the corrective, detective and preventive actions to mitigate Risk. Preventive controls keep errors or irregularities from occurring; detective controls detect errors and irregularities, which have already occurred and ensured their immediate correction. Corrective controls help to mitigate damage once a risk has materialised. This means that the level of attack determines the type of control used, and the effectiveness of the existing controls is evaluated. The CIS_CSC recommended a list of controls that we adopt for the proposed framework. This means that the level of attack determines the type of control to be used and the effectiveness of the existing controls. To evaluate the effectiveness of the existing controls, an assessment of each control objective is carried out. We apply a set of criteria: Relevance- The level to which the control addresses the relevant control objectives under analysis. Strength- The strength of the control is determined by a series of factors. Coverage means the levels at which all significant risks areaddressed. Integration- The degree and manner in which the control reinforces other control processes for the same objective—traceability- How traceable the control is, which allows it to be verified subsequently in all respects. The sub-class is *control type* and *control effectiveness.*

The Meta-model, illustrated in figure 2 shows the relationship between the concepts. An actor represents an entity, an organisation or a human user that generates strategic, operational and tactical plans within its organisational setting. Identifying actors is essential for determining the roles played by actors and the implementation of the framework's process. An actor owns a wide range of assets that require several security goals for supporting the business process. As a result, critical assets to operations are comprehensively profiled to include the security goal every asset must achieve, the business process supported by assets, and, importantly, each asset's criticality to the organisation. The Actor is represented as having an interest in the organisation's assets. These assets have security goals such as confidentiality, integrity and Availability for the business's continuation and reputation, and the attainment of one or more of the goals is always their focus. The Actor has complete control

Figure 2. A meta-model for i-CSRM at an organisational level


Plan
-Strategic: String
-Operational: String
-Tactical: String
is-obligatedTo-performActionOn(Risk)
Goals
-Type:String
-is-obligatedTo-PerformActionOn(Actor)
-is-obligatedTo-ProtectActorOf(Actor
-has-assestOf(Assets)
Actor
-Type: String
-Role: String
-is-obligatedTo-generateActionOn(Report)
-is-permittedTo-performActionOn(Risk)
-has-AssetsOf(Asset)
-has-PlansOf(Plan)
-has-RoleToProtect(Asset)
-is-AffectedBy(Risk)
Asset
-Type: String
-Criticality: String
-Goals: String
-has-ConfidentialityLossValueOf(Goal)
-has-AvailabilityLossValueOf(Goal)
-has-IntegrityLossValueOf(Goal)
-has-ConformanceLossValueOf(Goal)
-has-AccountabilityLossValueOf(Goal)
-has-FinancialLossValueOf(Goal)
-has-ReputationalDamagOf(Goal)
-has-VulnerabilityOf(Vulnerability)
-is-AttackedByThreat-ActorOf(Threat-Actor)
-is-ThreatendByThreatOf(Threat)
Threat Actor
-Opportunity: String
-Motivation: String
-Skill: String
-Resources: String
-Location: String
-Size: String
-exploits-VulnerabilityOf(Asset)
-impersonates(Actor)
-targets-AssetsOf(Actor)
-causes-RiskTo(Actor)
-requires-SkillLevelTo-PerformAttackOn(Actor)
-requires-ResourceTo-PerformAttackOn(Actor)
-requires-LocationTo-PerformAttackOn(Actor)
-uses-TTPTo-performAttackOn(Actor)
Indicator
-Type
-specifies-TTPOf(TTP)
-indicates-ThreatActorOf(Threat-Actor)
-affects-AssetOf(Asset)
Risk
-Type: String
-Level: String
-perform-ActionOf(Threat)
-peform-ActionOfVulnerability)
-requires-ControlOf(Controls)
-affects-AssetsOf(Assets)
-affects-
Vulnerability
-Type: String
-Targetted assets: String
-Rating: Integer
-leadsTo-ThreatOf(Threat)
-causes-RiskOf(Risk)
Incident
-Affected Assets: String
-Related TTP: String
-Nature of Compromise:String
-Controls requested/taken:String
-Impact assessment
-Time-related information:
-targets-AssetOf(Asset)
-affects-AssetOf(Asset)
-is-influencedBy-RiskOf(Risk)
-has-attributedThreat-actorOf(Threat-Actor)
-has-NatureOfCompromiseOf(Indicator)
-has-responseOf(Control)
-has-related(Indicator)
Controls
-Type: String
-addresses-RiskTo(Risk)
-mitigates-ThreatsOf(Threat)
-reduces-VulnerabilityOf(Asset)
-performs-ActionOf(Risk)
TTP
-Tactics: String
-Techniques: String
-Procedures: String
-perform-AttackOn(Asset)
-exploits-VulnerabilityOf(Vulnerability)
-causes-RiskOn(Actor)
-usedBy-Threat-ActorOf(Threat-Actor)
Threat
-Type: String
-Related Vulnerability: String
-Target asset: String
-exploit-VulnerabilityOf(vulnerability)
-is-causedByVulnerabilityOf(Vulnerability
-is-influncedByVulnerabilityOf(Vulnerability)
introduces
implement
have
affects
has
attacks
affects
results to
have
uses
generates
specifies
requires
addresses
exploits
influences
mitigates
1..*
0..*

over its assets and needs to keep the assets secure for its continuity, but these assets are prone to weaknesses in their systems, known as vulnerabilities. Vulnerability is the weakness or mistake in an organisation's security program, software, systems, networks, or configurations targeted and exploited by a threat actor to gain unauthorised access to an asset (system or network) using TTP. When not addressed on time, these vulnerabilities can lead to a threat that introduces Risk, and this Risk is likely to lead to the exploitation of the assets. Risk is the failure of an organisation or individual to achieve its goals due to the malicious attempt to disrupt its critical services by a threat. Organisations cannot wholly avoid Risk; however, it is the actors' role to ensure that risks are kept to a minimum level to achieve the goals by integrating CTI to improve i-CSRM. Therefore, the different controls regarding security and the organisation are introduced to help mitigate the risks.

The threat actor is a type of Actor with malicious intent characterised by their identity, suspected motivation, goals, skills, resources available for them to carry out a successful attack, past activities, TTP used to generate a cyber-attack and their location within the organisation's network. They try to impersonate actors by deceiving users of the critical infrastructure into believing them and then getting hold of some sensitive information or directly compromising their critical assets and leading to a significant risk to the organisation. This is done when vulnerabilities in an asset of the organisationare exploited using some TTP. A threat actor uses TTP to plan and manage an attackby following a specific technique and procedure.

They involve the pattern of activities or methods associated with a specific threat actor and consist of the threat actor's specific behaviour (attack pattern) and specific software tools that threat actors can use to perform an attack leaving behind the attack's incident. The incident is the type of event that represents information about an attack on the organisation. Some specific components determine the type of incident, such as; threat types, threat actor's skill, capability and location, assets affected, parties involved, and time. With a specific attack pattern, the organisation tends to think broadly by developing a range of possible outcomes to increase their readiness for a range of possibilities in the future. With Indicators, a pattern that can

Table 1. Relationship between concepts

Source	Type	Target
Actor	Generates	Report
Actor	Needs	Assets
Threat actor	Impersonates	Actor
Threat actor	Exploits	Vulnerability
Threat actor	Uses	TTP
Threat actor	Generates	Incident
Threat actor	Attacks	Assets
Incident	Affects	Actor
Incident	Results to	Risk
Incident	Affects	Asset
Incident	Influenced by	Threat
Vulnerability	Influences	Threats
Controls	Addresses	Vulnerability
Control	Mitigates	TTP
Controls	Addresses	Threats
Controls	Mitigates	Incident
TTP	Exploits	Vulnerability
Indicator	Specifies	TTP
Indicator	Indicates	Threat actor
Indicator	Generates	Incident
Risk	Requires	Control
Risk	Affects	Actor
Risk	Requires	Control
Threat	Introduces	Risk

be used to detect suspicious or malicious cyber activity is gathered. Table 1 shows the relationship between all the concepts.

PROCESS FOR THE INTEGRATED CYBERSECURITY RISK MANAGEMENT (I-CSRM) FRAMEWORK

This section presents an overview of the underlying process involved in the i-CSRM framework. Primarily, the process aims to introduce different phases of activities that organisations can follow for understanding and managing risks by looking at essential considerations such as identifying roles, assessing critical assets, identifying vulnerabilities and threats, assessing risks, and evaluating controls. The process also helps organisations understand the associated risks and the necessary control measures to align with the business goals. The process helps organisations build a risk management profile from scratch to the end, meaning that they will provide accurate information about risks based on the context and validate whether expectations are being met by the organisation continuously. Therefore, the principal beneficiaries of the framework and its process are organisations that provide critical infrastructures responsible for ensuring the security of a given nation, its economy, and the public's health and safety and data protection. Hence, it is essential to emphasise that the framework does not focus on individual users who usually do not have as much obligation towards overall security, diverse requirements and responsibilities as organisations.

An essential aspect of the process is that it provides systematic activities for developing an efficient risk management approach that is mainly security-oriented and provides a roadmap for organisations to achieve overall cybersecurity. The process's core includes several diverse activities and steps to help guide key decision points about organisational context, threat and vulnerability activities, potential risks, and security controls. It helps identify and interlink risk management components for ensuring efficiency, effectiveness and consistency within different areas of the organisation.

Another essential feature of the process is that most of the activities are designed by considering various leading industry best practices, frameworks, guidelines, and standards applicable to all organisations regardless of their size or the domain in which they operate. This implies that the process is all-encompassing in nature and not tailored to a specific organisation type or solution but built upon high-level considerations to ensure important cybersecurity issues are not overlooked.

Table 2. i-CSRM framework process

Activity	Steps	Input	Technique	Performed by	Output
Activity 1: Organisational Context	Identify actors and their roles	They are grouping the actors into internal and external. Internal actors represent the respective roles and responsibilities of personnel/departments within an organisation. External actors include stakeholders that are involved in the delivery of other services outside the organisation	Examining job profile, roles, duties and responsibilities of actors	Top management	A defined list of actor and their roles
Activity 2: Asset Identification and Criticality	Asset Profiling	An overview and list of the organisation's assets, their core functionalities and subcomponents.	Review of asset inventory, security policy, interviewing security analyst and physical observation of assets	Security Analyst and IT Manager	Description of assets, functions, and subcomponents owners, criticality and asset goals
	Identify the Asset security goals	Existing asset profile	Combination of asset control principles and organisation's security policies	Security Analyst	Enumeration of security goals and principles that each asset must achieve for sustained operations of the organisation
	Determine Asset criticality	Asset profile and goals.	Employing asset criticality ranking using fuzzy logic to determine criticality level	Security analyst	Consistent and unambiguous classification of assets according to criticality level to the organisation's processes and functions.
Activity 3: Threat Modelling	Determine Vulnerability profile	Organisational assets and list of vulnerabilities provided by CWE	Employing CWE methodology for vulnerability ranking	Security Analyst	A comprehensive vulnerability profile ranking vulnerabilities in assets according to the CWE methodology
	Determine Threat profile	Organisational assets, list of threats provided by CAPEC	Employing the CAPEC model for threat analysis	Security Analyst	A comprehensive threat profile detailing potential threats to assets according to the ATT&CK model
Activity 4: Risk Assessment	Predict Risk Types	A collection of security risks from OWASP that are associated with the threats are identified	Application of OWASP risk methodology that provides a list of risk types	Security Analyst	A detailed risk register highlighting risks types
	Risk level prediction	A collection of vulnerabilities and list of critical asset, potential threats identified and existing control measures are provided from CAPEC	Application of machine learning technique that estimates risks type and risk level	Security Analyst	A detailed risk register highlighting risks type and risk level and recommended controls

Continued on following page

Table 2. Continued

Activity	Steps	Input	Technique	Performed by	Output
Activity 5: Risk Controls	Identify Existing Controls	A list of organisations controls detailing control functionalities	Review of control inventory and report of existing control measures	Security Analyst	A detailed control register highlighting existing controls
	Determine the effectiveness of existing Controls	The result of findings based on examining and analysing existing controls and implementing new controls from CIS CSC	Manual and automated documentation of findings	Security Analyst	A detailed control register highlighting existing controls and a list of new controls

Activity 1: Organisational Context

Every organisation exclusively operates within a defined scope and available resources. Organisational context tends to better understand the organisation's existing state by providing the essential elements of information needed to give an i-CSRM framework proper direction to be achieved successfully. The organisational context involves identifying its significant stakeholders, actors, critical assets, security goals and how they impact risk management and viability. A stakeholder is any entity with a conceivable interest or stake in an activity (Goodpaster, 1991). A stakeholder can be an individual, group of individuals, or an institution affected by or influences an activity's impact. Stakeholders are actors such as top management and administrators. Who are directly or indirectly involved in influencing the success of the organisation and its processes.To successfully execute the process and achieve this activity, it is essential to obtain a comprehensive picture of actors and their roles in meeting requirements. This becomes important in identifying and avoiding a potential conflict of interests and other issues such as the actors responsible for the security and maintenance of organisations assets.

Step 1: Identification of Actors and Their Roles

An actor represents an entity such as an organisation or human user with a strategic goal within its organisational setting, carries out specific activities and makes informed decisions. Actors interact with the organisation's systems or relationshipsby providing technical and nontechnical support or services to the organisation. The nature of communications between actors needs to be clearly balanced, reconciled, interpreted and managed accordingly. The organisation's activities require an active set of actors to carry out various tasks to guide and lead the organisation in achieving its goals and ensuring its successful operations. In this case, actors can be identified as internal and external actors. The internal actor is the organisation itself that supply infrastructure, network facilities and other services needed to run its operations and has skilled personnel who play different roles such as information technology security analyst, risk manager and senior engineer. External actors mainly include users who use the organisation's services and third-party vendors who provide other services such as internet services.

Activity 2: Asset Identification and Criticality

This activity aims to identify and prioritise assets in terms of their boundary, components and assigning weights to the assets based on the organisation's importance. Assets are specific units such as hardware, a database, application, or program that support the delivery and usage of an organisation's services.

Furthermore, to support organisations in assessing each asset's criticality, a decision support system using fuzzy set theory is created. A fuzzy set theory provides a way of absorbing the uncertainty inherent to phenomena whose information is unclear and uses a strict mathematical framework to ensure precision and accuracy and the flexibility to deal with both quantitative and qualitative variables (Zimmermann, 2011). It can be used for approximate reasoning, easy to implement and adopt individual perception without incurring complexity within the risk management process. This activity includes three steps; identify assets and their goals, determining asset criticality, and identifyingthe business process. The resulting critical asset list is then used to assess vulnerability assessment and threat identification in Activity 3.

Step 1: Asset Profile

This step's basis is to profile assets in terms of their components, boundaries and assigning weight to the assets based on assets vital to the organisation. Assets are specific units such as a database, application, or program that support the delivery and usage of an organisation's services. To create asset profiles, a Security Analyst is involved in identifying assets by considering the core functions of the assets, alongside other subcomponents essential to achieving and maintaining crucial functions. Important asset information can be gathered by reviewing background materials, including independent audit/analytical reports, interviewing the critical infrastructure users, and physical observation of organisational assets. Besides, asset specification and management documentation provide essential details about the organisational asset.

Step 2: Identify Asset Security Goals

Security asset goals are specific attributes that describe assets expected conformance to secure behaviour: they are also referred to as security principles. Identifying assets security goals is vitalfor an organisation to determine what critical views of security must be ensured by each asset during processing, storage, or transmission by authorised systems, applications, or individuals. Also, asset security goals are used in determining the impact that may result from accessing assets in an unauthorised manner for use, interruption, change, disclosure. Therefore, the Security Analyst considers a set of security goals that each asset aims to achieve. The consequential impact that may ensure the compromise of the security goals and the level of protection needed can be easily determined. There are different asset categories we consider for asset criticality. They include; software, data, hardware, information communications and network and people. We further defined a set of asset security goals every asset must aim to achieve, such as;

- **Asset Availability (A):** Availability refers to ensuring that an asset is made available and accessible to authorised users when and where they need it.
- **Asset Integrity (I):** Asset integrity refers to an asset's ability to perform its required functions effectively and efficiently without disrupting or losing its services.
- **Asset Confidentiality (C):** Asset confidentiality refers to assets staying secured and trusted and preventing unauthorised disclosure of sensitive data.
- **Accountability (ACC):** This asset goal requires that attack or incident actions that occur on an asset are tractable to the responsible system or actor.
- **Conformance (CON):** This asset goal ensures that the assets such as services meet the specified standard.

Step 3: Determine Asset Criticality

This step aims to identify and prioritise an organisation's critical asset by assessing those assets' primary security goals. In other words, the criticality of each asset is based on its relative importance. Asset criticality is imperative for prioritising and developing actions that will reduce risks to the asset, improve asset reliability, and define strategies forimplementing the appropriate controls. To ensure validity, consistency, and support stakeholders in assessing each asset's criticality, a decision support system using fuzzy set theory is created. Fuzzy set theory plays a vital role in the decision process enhancement. It helps to deal with or represent the meaning of vague concepts, usually in situation characterisation such as linguistic expressions like "very critical". Fuzzy logic, introduced by (Zadeh, 1988), is one of the best ways to deal with all types of uncertainty, including lack of knowledge or vagueness (Markowski & Mannan, 2009). This system provides a methodology for computing directly with the word. Fuzzy set theory is a generalisation of classical set theory that provides a way to absorb the uncertainty inherent to phenomena whose information is vague and supply a strict mathematical framework to ensure precision and accuracy, as well as the flexibility to deal with both quantitative and qualitative variables (Zimmermann, 2011).

Development of a Fuzzy Asset Criticality System (FACS)

Criticality is the primary indicator used to determine the importance of the assets to the organisation. After the different assets have been identified, we determine the criticality based on their relative importance using Fuzzy Asset Criticality System (FACS).

- **Fuzzification:** FACS determines asset criticality by using (C, I, A, CON and ACC) as the five fuzzy inputs for assessing the criticality of individual assets and assigning a level of criticality. Each input is assigned five fuzzy labels Very Low (VL), Low (L), Medium (M), High (H) and Very High (VH), for assessing the level of the fuzzy output Asset criticality (AC) value which is assigned five fuzzy labels Very Low Critical (VLC), Low Critical (LC), Medium Critical (MC), High Critical (HC) and Very High Critical (VHC) of individual assets. The details of fuzzy sets applied in the first step of the fuzzy inference system are presented in Table 3.

Table 3 shows the numerical ranges in which fuzzy sets are selected based on them. The membership functions for AC also are depicted on a scale of 1 to 5. Figure 3 shows the structure of the FACS.

- **Rules:** There are many fuzzy inference methods; however, this research uses the Min-Max fuzzy inference method proposed by Mamdani (Cordón, 2011). This research employs Mamdani's method due to several advantages (Cord, 2001):
  - It is suitable for engineering systems because its inputs and outputs are real-valued variables
  - It provides a natural framework to incorporate fuzzy IF-THEN rules from human experts
  - It allows for a high degree of freedom in the choices of fuzzifier, fuzzy inference engine, and defuzzifier so that the most suitable fuzzy

Table 3. Fuzzy ratings

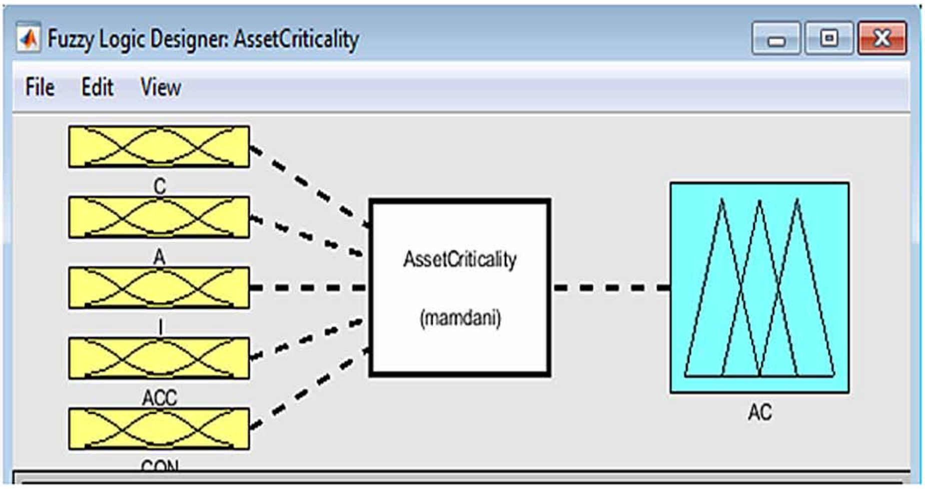
Features	Asset Factors	Description	Linguistic Terms	Crisp Rating	Interpretation
Input	Confidentiality (C)	How much data could be disclosed, and how sensitive is it?	Very High (VH)	5	All data disclosed
			High (H)	4	Extensive critical data disclosed
			Medium (M)	3	Extensive non-sensitive data disclosed
			Low (L)	2	Minimal critical data disclosed
			Very Low (VL)	1	Minimal non-sensitive data disclosed
	Availability (A)	How many services could be lost, and how vital is it?	Very High (VH)	5	All services completely lost
			High (H)	4	Extensive primary services interrupted
			Medium (M)	3	Extensive secondary services interrupted
			Low (L)	2	Minimal primary services interrupted
			Very Low (VL)	1	Minimal secondary services interrupted
	Integrity (I)	How much data could be corrupted,and how damaged is it?	Very High (VH)	5	All data corrupt
			High (H)	4	Extensive seriously corrupt data
			Medium (M)	3	Extensive slightly corrupt data
			Low (L)	2	Minimal seriously corrupt data
			Very Low (VL)	1	Minimal slightly corrupt data
	Accountability (ACC)	Are the threat actors traceable to an individual?	Very High (VH)	5	Completely anonymous
			High (H)	4	Fully traceable
			Medium (M)	3	Highly traceable
			Low (L)	2	Possibly Traceable
			Very Low (VL)	1	Minimal Traceable
	Conformance (CON)	How much deviation from specified behaviour constitutes conformance?	Very High (VH)	5	Full variation
			High (H)	4	High profile variation
			Medium (M)	3	Clear variation
			Low (L)	2	Low variation
			Very Low (VL)	1	Very low variation

Continued on following page

Table 3. Continued

Features	Asset Factors	Description	Linguistic Terms	Crisp Rating	Interpretation
Output	Asset Criticality (AC)	How critical is the asset to the organisation?	Very Critical (VC)	5	Extremely critical and is of high value to the CI organisation, it requires an extreme level of protection
			Highly Critical (HC)	4	High importance to the organisation and requires a high level of protection.
			Medium Critical (MC)	3	The asset is moderately important to the organisation and requires moderate protection
			Low Critical (LC)	2	The asset is of minimal importance and does not require many levels of protection.
			Very Low Critical (VLC)	1	The asset non-critical and requires a very low level of protection

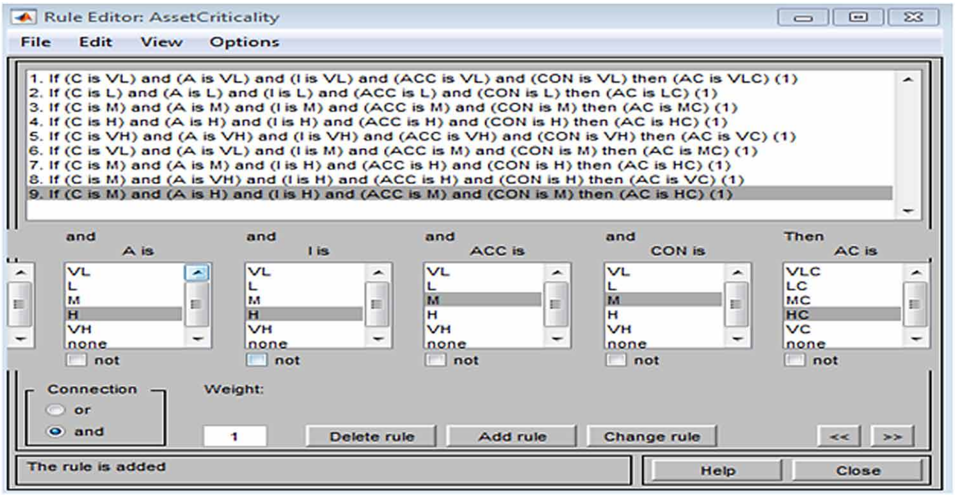
Figure 3. Structure of the fuzzy asset criticality system (FACS)



logic system for a particular problem is obtained. It provides a natural framework to include expert knowledge in the form of linguistic rules.

We used 125 IF-THEN rules to provide a database by mapping five input parameters (C, A, I, CON and ACC) and AC value. The rules are designed to follow the logic of the Asset criticality evaluator. A number of the IF-THEN rules of the developed system are shown in Figure 4.

Figure 4. Rules set for FACS



Rule Editor: AssetCriticality

1. If (C is VL) and (A is VL) and (I is VL) and (ACC is VL) and (CON is VL) then (AC is VLC) (1)
2. If (C is L) and (A is L) and (I is L) and (ACC is L) and (CON is L) then (AC is LC) (1)
3. If (C is M) and (A is M) and (I is M) and (ACC is M) and (CON is M) then (AC is MC) (1)
4. If (C is H) and (A is H) and (I is H) and (ACC is H) and (CON is H) then (AC is HC) (1)
5. If (C is VH) and (A is VH) and (I is VH) and (ACC is VH) and (CON is VH) then (AC is VC) (1)
6. If (C is VL) and (A is VL) and (I is M) and (ACC is M) and (CON is M) then (AC is MC) (1)
7. If (C is M) and (A is M) and (I is H) and (ACC is H) and (CON is H) then (AC is HC) (1)
8. If (C is M) and (A is VH) and (I is H) and (ACC is H) and (CON is H) then (AC is VC) (1)
9. If (C is M) and (A is H) and (I is H) and (ACC is M) and (CON is M) then (AC is HC) (1)

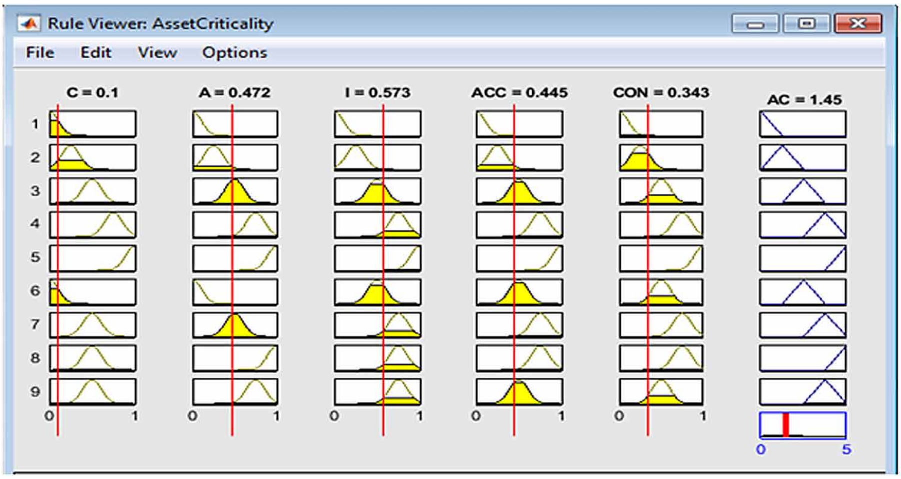
and A is: H
and I is: H
and ACC is: M
and CON is: M
Then AC is: HC

Connection: ○ or ● and

Weight: 1

The rule is added

Figure 5. Sample of rules



- **Inference Engine:** An inference engine attempts to create solutions from the database. In this paper, the inference engine maps fuzzy input sets (C, A, I, ACC and CON) into fuzzy output set (AC). Figure 5 shows several IF-THEN rules to provide a more understanding of the proposed FACS model.
- **Defuzzification:** Different methods for converting the fuzzy values into crisp values such as Centre of Gravity (COG), Maximum Defuzzification Technique and Weighted Average Defuzzification Technique. One of the most commonly used defuzzification methods is COG. The COG technique can be expressed as follows:

$$X^{*} = \frac{\int \mu_{i}(x)xdx}{\int \mu_{i}(x)dx} \tag{1}$$

Where x* is defuzzified output, μi(x) is aggregated membership function, and x is the output variable.

A table of asset inventory is therefore, displayed showing the critical level for each asset.

Activity 3: Threat Modelling

Threat modelling activity focuses on identifying and measuring vulnerabilities and threats related to the assets. The Security Analyst performs this activity. Based on the previous activity's assets, all possible threats that could impact the assets negatively are profiled in a register. However, effective identification and control of threats require an understanding of threat sources, threat actor behaviour, capability and intent (Workman et al., 2008). Only through an understanding of the current threat landscape can organisations know about the nature of threats they face and the control measures to implement. In other words, a holistic understanding of threats enables a more effective prioritisation of control actions and decision making. This is possible when known attack patterns employed by the threat actor to exploit vulnerabilities are known to allow an organisation to understand and create a threat profile expansively. Because of these considerations, this activity has created two steps for threat modelling: (i) the determination of Vulnerability profile; and (ii) the determination of threat profile.

Step 1: Determine the Vulnerability Profile

Determining the vulnerability profile is vital because it allows for identifying and assessing vulnerabilities associated with critical assets. This step aims to identify potential asset vulnerabilities that a threat actor may leverage to exploit an asset. It is an essential and delicate task that has an impact on the successful operation of critical infrastructures. A sound approach that enables gathering valuable insights based on the analysis of situational and contextual vulnerabilities that can be tailored to the organisation-specific threat landscape is used.

Hence, the Common Weakness Enumerator (CWE) methodology (Martin, 2007) is used to determine the vulnerability factors as a publicly known vulnerability source. Therefore, to estimate the likelihood of risk, it is necessary to estimate a particular vulnerability discovered and exploited. We adopt CWE, which allows for weaknesses to be characterised, allowing stakeholders to make informed decisions when mitigating risks caused by those weaknesses. Each related weakness is mapped to CAPEC and identified by a CWE identifier and the name of the vulnerability type. The CWE gives a general description, behaviour, likelihood of exploit, consequences of exploit, potential mitigation and related vulnerabilities. To apply the CWE methodology, a rating table is presented in table 5.4 with corresponding values assigned to the different factors that can help organisations determine the likelihood of risk. Each option has a likelihood rating from 0 to 9, and the overall likelihood falls within high, medium and low, which is sufficient for the overall risk level. The Security Analyst could explore other publicly available sources of vulnerability information,

Table 4. Vulnerability factor rating

Vulnerability Factors	Vulnerability ID	Description	Likelihood Rating	
			Weight	Value
Ease of discovery	EoD	How easy is it for vulnerability to be discovered?	1	Practically impossible
			3	Difficult
			7	Easy
			9	Automated tools available
Ease of exploit	EoE	How easy is it for vulnerability to be exploited?	1	Theoretical
			3	Difficult
			5	Easy
			9	Automated tools available
Awareness	Awa	How well known is this vulnerability to the threat actors?	1	Unknown
			4	Hidden
			6	Obvious
			9	Public knowledge
Intrusion detection	I_D	How likely is an exploit to be detected?	1	Active detection in application
			3	Logged and reviewed
			8	Logged without review
			9	Not logged

including internal experience, penetration test, vulnerabilities catalogues available from industry bodies, national government, and legal bodies. The questions can also be extended to meet the organisation's need.

Step 2: Determine Threat Profile

Determining the threat profile is essential because it allows for the identification and understanding of threat characteristics. To determine threats, it requires a structured representation of threat information that is expressive and all-encompassing due to the dynamic and complex nature of a CPS. A Security Analyst must use a sound approach that enables gathering valuable insights based on the analysis of situational and contextual threats that can be tailored to the organisation-specific threat landscape. A method that could be used is MITRE's models for the threat intelligence sharing called CAPEC and WASC. Therefore, this step effectively identifies the threat types, target assets, threat actor factors, TTP, and compromise indicators likely to affect a critical infrastructure's ability to deliver its services.

CAPEC is an acronym formed from the first letter of Common Attack Pattern Enumeration and Classification used to define the potential threat, provide context for architectural risk analysis, and understand trends and attacks to monitor. Also, WASC stands for Web Application Security Consortium. Hence, the Security Analyst could explore publicly available sources of threat information. For example, we recommend that threat information approved by CAPEC (Barnum, 2008) and WASC (Consortium, 2009) be followed because there are several threats identified in these two sources. Besides using the CAPEC and WASC models, actors use the following procedure to create a comprehensive threat profile:

- **Threat type:** To create a comprehensive threat profile, organisations need to identify the potential threats of assets that a threat actor may leverage to attack. The Security Analyst needs to back up his claim with a solid foundation of Information sources.
- **Threat Actor factors:** Effective identification and control of threats require an understanding of threat sources, threat actor behaviour, skill, resources required, capability and intent (Workman et al., 2008). Therefore, we adopt the OWASP methodology that considers various threat actor factors such as; skill level, size, motivation, location, resources, and opportunity to understand the attack and its trend. Using these threat actor factors, the Security Analyst can determine the likelihood of an attack and the severity of the threat. This will provide the ability to create an impact rating for threats. Table 5 shows the threat actor factors, and each factor has a set of options with a likelihood rating from 0-9.

Table 5. Threat actor factors rating

Threat Actor Factors	Description	Likelihood Rating	
		Weight	Value
Skill level	How technically skilled is the threat actor?	1	No technical skills
		3	Some technical skills
		5	Advanced computer user
		6	Network and programming skills
		9	Security penetration skills
Location	Through what channel did the threat actor communicate to reach the vulnerability?	1	Internet
		8	Intranet
		8	Private Network
		7	Adjacent Network
		5	Local Network
		2	Physical
Motive	How motivated is the threat actor to find and exploit the vulnerability?	1	Low or no reward
		4	Possible reward
		9	High reward
Resources	What resources are required for the threat actor to find and exploit the vulnerability?	0	Expensive resources required
		4	Special resources required
		7	Some resources required
		9	No resources required
Opportunity	What opportunities are required for the threat actor to find and exploit the vulnerability?	0	Full access required
		4	Special access required
		7	Some access required
		9	No access required
Size	How large is the group of the threat actor?	2	Developers
		2	Systems administrators
		4	Intranet users
		5	Partners
		6	Authenticated users
		9	Anonymous internet users

- **Determine Tactics, Techniques and Procedures (TTP) and Indicator of Compromise (IOC):** TTP and IOC involve the pattern of activities used by a threat actor to plan and manage a cyber attack, thereby compromising critical assets. The different TTP types include; *initial access, execution, credential* *access, persistence, privileged escalation, defence evasion, collection, lateral movement, exfiltration* and *command and control*. The different IOC includes; *network indicators, email indicators* and *host indicators.* Therefore, we adopt the ATT&CK (adversarial tactic, techniques and common knowledge) framework developed by MITRE to document standard TTP used to target, compromise and operate in an enterprise network. To calculate the risk level and know the appropriate controls to protect the organisation's assets, information about TTP must be known. Table 6 shows the possible TTP and IOC that are frequently employed when exploiting the vulnerability.

Table 6. TTP and IOC (Tactic, 2017)

Tactics Type	Techniques	Procedure	IOC
Initial access	Spearphishing link	It employs links to download malware in an email by electronically delivering social engineering targeted at a specific individual or organisation.	Email, Network
	Drive-by compromise	A threat actor gains access to a system by visiting a website over the ordinarybrowsing course. The website is compromised where the threat actor has injected some malicious code.	Network
	Replication through removable media	The threat actor uses a tool to infect connected USB devices and transmit them to air-gapped computers when the infected USB device is inserted.	Host
	Spearphishing attachment	A threat actor attaches and sends a Spearphishing email with malicious Microsoft office attachment and requires user execution in other to execute.	Email
Execution	Command-line interface	The threat actor uses a command-line interface to interact with systems and execute other software during operation.	Host
	Dynamic data exchange (DDE)	Threat actor sends a Spearphishing containing malicious word document with DDE execution.	Host, Network
	Execution through module load	The threat actor uses this functionality to create a backdoor through which it can remotely load and call dynamic link library (DLL) functions.	Host
	Exploitation for client execution	Threat actor exploits a vulnerability in office applications, web browsers or typicalthird party applications to execute the implant into the victim's machines.	Network

Continued on following page

Table 6. Continued

Tactics Type	Techniques	Procedure	IOC
Persistence	Account manipulation	Threat actor adds a created account to the local administrator's group to maintain elevated access.	Host, Network
	Accessibility features	The threat actor uses a combination of keys known as the sticky keys to bypass a user's windows login screen on remote systems during the intrusion.	Host, Network
	Component firmware	Threat actor overwrites the firmware on a hard drive by compromising computer components.	Host, Network
Privilege escalation	External remote services	Threat actors leverage legitimate credentials to log into external remote services	Host, Network
Defense evasion	Disabling security tools	Threat actor disables the windows firewalls and routing before binding to a port.	Host, Network
Credential access	Brute force	Threat actor brute forces password hashes to be able to leverage plain text credentials.	Host, Network
Discovery	Network sniffing	The threat actor uses a tool to capture hashes and credentials sent to the system after the name services have been poisoned.	Host, Network
	Network service scanning	Threat actor used BlackEnergy malware to conduct port scans on a host.	Host
	System information discovery	The threat actor uses tools such as systeminfo that obtains information about the local system.	Host
Lateral movement	Remote services	The threat actor uses putty secure copy client (PSCP) to transfer data or access compromised systems.	Host
	Third-party software	Threat actor distributes malware by using a victim's endpoint management platform.	Host
Collection	Data from information repositories	Threat actor collects information from Microsoft SharePoint services using a SharePoint enumeration and data dumping tool within target networks	Host, Network
	Email collection	The threat actor uses utilities to steal email from archived outlook files and exchange servers that have not yet been archived.	Email, Host, Network
	Man in the browser	The threat actor uses a Trojan spyware program to perform browser pivot and inject into a user's browser and trick the user into providing their login credentials on a fake or modified web page.	Network
Exfiltration	Data encrypted	The threat actor uses malware such duqu to push and execute modules that copy data to a staging area, compress it, and XOR encrypts it.	Host

Continued on following page

Table 6. Continued

Tactics Type	Techniques	Procedure	IOC
Command and control	Commonly used port	The threat actor uses duqu, which uses a custom command and control protocol that communicates over commonly used ports and is frequently encapsulated by application layer protocols.	Network
	Remote file copy	The threat actor used Shamoon malware to download an executable to run on the victim.	Network

A table displays the threat profile showing the output of the threat modelling activity used as an input for the risk assessment activity.

Activity 4: Risk Assessment

The output of threat modelling provides a list of vulnerabilities, related vulnerabilities, potential security threats, and assets' impact. The threat register serves as a help to the Security Analyst to orchestrate a risk register's creation and focus on the most potent threats. This activity allows for establishing the risk assessment context by following the threat register and formally approves the risk management activities within the organisation. The activity provides various additional estimations required for the risk evaluation by enabling the determination of risks that are likely to occur, the severity of the risks, and the steps to control or manage the risks. This requires the top management and risk manager's active involvement to emphasise the importance of risk assessment to the organisation. This activity's output is a risk register, and the overall risk impact level falls within high, medium and low. This ensures that minor risks are not prioritised, while more severe risks are overlooked. The first step of this activity identifies risk types. Secondly, it identifies existing controls and lastly calculates risk impact value.

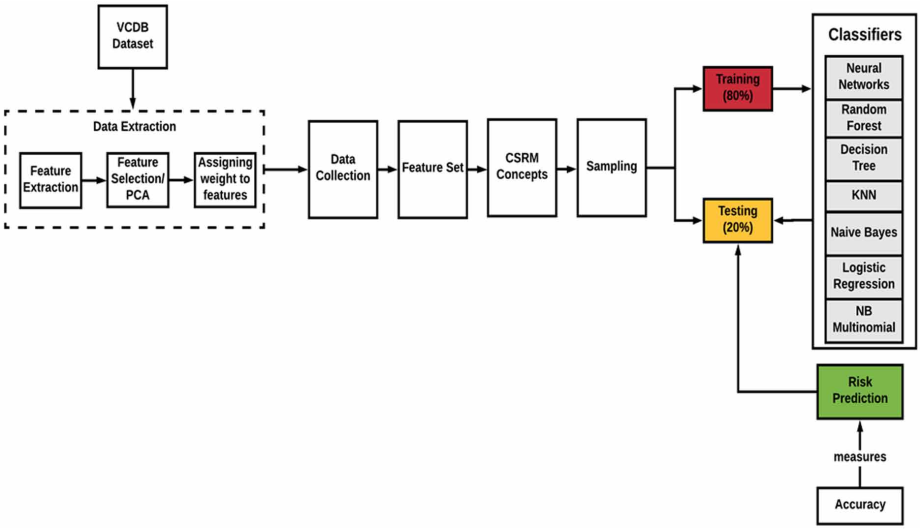
Step 1: Predict Risk Types

This step proposes using machine learning techniques for predicting risk type so that appropriate mitigation processes can be implemented. In this context, risk type prediction relies on a pioneering mathematical model such as machine learning for analysing, compiling, combining and correlating all incident-related information and data acquired from previous activities. The machine learning (ML) techniques automatically find valuable underlying patterns within i-CSRM concepts used as features, and then the patterns predict risk types. The i-CSRM features are considered input for the ML classifiers and ML classifiers to predicate the risk type. Therefore, we used well-known classifiers such as K-Nearest neighbours (KNN), Naïve Bayes (NB), the Naïve Bayes Multinomial (NB-Multi), Neural Network (NN) with Ralu activation function at activation layers and sigmoid function at the output layer, Decision Tree (DT), Random Forest (RF), and Logistic Regression (LR) for risk type prediction.

We present data extraction to generate a feature set, which is then further used on the ML classifiers for training purposes. Finally, the test data is used to check the accuracy of the prediction. Figure 6 shows how these features are used to train the classifiers and the step by step process of the risk prediction, i.e. the experiment in general. Data collection and extraction were considered from the dataset; feature extraction was carried out on those data and used to train the ML classifiers (NN, RF, LR, NB-Multi DT, KNN and NB). The data were further partitioned into 80% training and 20% testing. We used the widely known 10-fold cross-validation scheme to split the given data into testing and training set and reported the average results obtained over the ten folds. Predictions are carried out on the testing dataset, and accuracy measures the prediction.

Also, risks types from multiple industry bodies can be considered because they maintain a regularly updated list of most pressing security risks. For example, the Common Attack Pattern Enumeration and Classification (CAPEC) provide a comprehensive list of risks that can be used for understanding and enhancing defense. All these sources can be used.

Figure 6. Classification process about the primary analysis and methods that have been used to build the experiment



Step 2: Determine Risk Level

After information about the potential risk types, threat, vulnerabilities and assets have been identified and gathered, and the next step is to determine the risk level of all the possible risk types predicted. The risk level is usually not known and not estimated correctly. In essence, organisations need to rate security risks that have been identified. Therefore, for the risk level to be estimated, we used the technical impact factors. The technical impacts factors are inclined toward an asset's security goals that include; confidentiality, integrity, availability, accountability, and conformance. Also, iinformation about the threat actor and vulnerability factors needs to be gathered. The aim is to provide a rough estimate of the risk level's magnitude if a risk occurs.

Phase 1: To estimate the overall (L) Likelihood of the risk, threat actor factors and vulnerability factors are put into consideration, as shown in equation 2. Each option has a likelihood rating from 0 to 9, as shown in table 4 and 5. The overall likelihood falls within high, medium and low, sufficient for the overall risk score. Table 7 shows the overall likelihood level.

$$L = \frac{TAF + VF}{2} \tag{2}$$

Where:

L= Likelihood
TAF = Threat Actor Factors,
VF = Vulnerability Factors

$$\text{TAF} = \text{SL} + \text{L} + \text{M} + \text{Res} + \text{Opp} + \text{S} / \text{n} \tag{3}$$

Where:

SL = Skill Level
L = Location
M = Motivation
Res = Resource
Opp = Opportunity
S = Size
n = total number of TAF factors (6)

$$VF = EoE + EoD + Aw + ID / n \tag{4}$$

Where:

EoE = Ease of Exploit
EoD = Ease of Discovery
Aw = Awareness
ID = Intrusion Detection
n = total number of VF factors (4)

Table 7. Overall likelihood rating

Likelihood	Rating
Low	0.00 – 2.99
Medium	3.00 – 5.99
High	6.00 – 9.00

Phase 2: To Estimate the overall ($Impact_F$) impact of a successful attack, we consider the total loss of the asset's goals, as shown in equation 5. Each factor has a set of options with an impact rating from 0 to 9, as shown in table 8.

$$Impact_F = {}^{AF}\!/_{n} \tag{5}$$

Where:

$Impact_F$= Impact Factor
AF = Asset Factors (L_C +L_ A +L_I +L_ ACC +L_ CON)
L_C = loss of Confidentiality
L_A = loss of Availability
L_I = loss of Integrity
L_ACC = loss of Accountability
L_CON = loss of Conformance
n = Total number of the Technical factors (5)

Table 9 shows the overall $Impact_F$ level.

Table 8. Impact factors

Impact Factors	0 to < 3 (Low)	3 to < 6 (Medium)	6 to 9 (High)
Loss of Confidentiality	Minor disclosure of critical assets	Critical assets are significantly affected	Highly critical assets are extensively affected
Loss of Integrity	Minor compromise of critical assets	Critical assets significantly compromised	All highly critical asset extensively compromised
Loss of Availability	Minor interruption of critical assets	Critical assets significantly interrupted	All critical assets extensively lost
Loss of Accountability	Threats are fully traceable	Threats are possibly traceable	Threats are completely untreatable
Loss of Conformance	A minor breach of compliance requirements	A significant breach of compliance requirements	All compliance requirements significant breached.

Table 9. Overall impact$_f$ rating

Likelihood	Rating
Low	0.00 – 2.99
Medium	3.00 – 5.99
High	6.00 – 9.00

Phase 3: Determine Risk Severity: To determine the risk level, we estimate the likelihood and impact are combined to calculate the overall severity of risk using equation 6.

$$R_{Level} = L * Impact_F \tag{6}$$

Where;

R_{Level} = the risk level
I = the impact of the asset goals
L= the likelihood of the attack occurring within a given time-frame

Overall risk severity is rated as high, medium, or low, as shown in Table 10.

Table 10. Overall risk level

Overall Risk level	
00 – 20	Low
21 - 45	Medium
46 – 65	High
66 – 81	Critical

Activity 5: Risk Controls

There is a need to identify and implement controls that can be used to address the risks. Risk controls are generic fundamental technical or procedural mechanisms that are used to manage security risks. This activity displays the current risk status for each risk event, together with their calculated risk values. The Security Analyst needs to identify the potential control measures that can be used to mitigate the risks based on the risk level. Therefore, risk assessment plays a critical role in this activity. The Security Analyst considers various industry standards that provide recommendations on basic security controls. For example, the Critical Security Controls (Mbanaso et al., 2019) publishes a set of 20 controls and best practice guidelines that organisations should adopt to control known computer security risks. Thus, we recommend that the Security Analyst selects risk control measures from the predefined list provided by a renowned industry guideline named CSC CIS to define control measures. CSC CIS provides 20 controls categorised into three prioritised and defence-in-depth set of best practices that are implementable and usable to mitigate attacks against systems and networks.

In selecting the controls, the security Analyst uses the matching process to compare the security control measures from the different standards and identify and filter controls that have similarities, i.e. controls that complement each other in terms of scope. The elements used for the comparison include the name of the control measure, type, and keywords. In such cases where control measures are the same, the Security Analyst should adopt CSC CIS controls. However, if there is no similarity, control measures from both CSC CIS and other standards should be adopted. This approach ensures that contents are compared more thoroughly and risk control actions consistently and easily identified. Therefore, this activity's primary objective is to specify essential risks controls and evaluate the effectiveness of the existing control measures that protect assets to ensure sufficient coverage in the management of critical infrastructure.

Step 1: Identification of Existing Control Types

There is a need to identify a list of existing controls that are in place to address risks before risk level is identified. Therefore, this step identifies the existing controls and categorises them into corrective, detective and preventive actions to mitigate the risk. The risk impact level will determine those not adequate controls so that new controls can be implemented.

Step 2: Evaluating the Effectiveness of Existing Controls

This step involves assessing the effectiveness of existing controls, determining each control's level, and avoiding unnecessary duplication of controls if existing controls are not adequate and new controls need to be implemented. Therefore, a check should be made to ensure that the controls are working correctly. If a control does not work as expected, this may cause vulnerabilities leading to risks. Consideration should be given to the situation where a selected control fails in operation, and therefore complementary controls are required to address the identified risk effectively. In assessing the effectiveness of existing controls and determining each control's level, an assessment of each control objective is carried out by an assessor team. The controls are evaluated in terms of relevance, strength, coverage, integration, and traceability according to ISO 27005:2011 standard *(GOST, 2009).* For each criterion, a rating score from 1 to 5 is given to measure which control addresses the specific control objective. Table 11 shows the five different criteria rating.

Table 11. Criteria rating

Rating		Description
5	Adequate control	The control achieves the objectives intended to mitigate the risks.
4	Adequate control with some areas of improvement	The control achieves the objectives intended to mitigate the risks with evidence of some areas, though not critical, subject to improvement to meet sound controls' requisites.
3	Generally adequate control, with some critical areas	The control mostly mitigates the risks intended to mitigate the risks. However, the characteristics of some of the controls are not entirely consistent with basic sound controls
2	Inadequate control, subject to significant improvement	The control partially achieves the control objectives intended to mitigate the risks
1	Insufficient control	The control is not sufficient to achieve the control objectives intended to mitigate the risks.

Table 12. Overall effectiveness

Description	Overall Effectiveness
Insignificant	0-5
Minor	6-10
Moderate	11-15
Major	16-20
Critical	21-25

Table 12 shows the overall effectiveness of the controls.
To find the overall evaluation of each control, equation 7 is given:

$$OE = R + S + C + I + T \tag{7}$$

Where:

OCE = Overall Control Effectiveness
R = Relevance
S = Strength
C = Coverage
I = Integration
T = Traceability

A table displays the control type together with its calculated overall control effectiveness value.

Step 3: Implement Control Measures to Determine New Risk Status

Table 13 presents the control measures implemented in three levels represented in three different colours. The green ones are fully implemented to reduce the risk value evenly. The yellow ones are only partially implemented and reduce the risk value by half of a green one. The red ones do not reduce the risk at all. Therefore, this step involves performing appropriate analysis to measure which control addresses which risk. Criteria, each criterion help the assessment; a rating score from 0 to 9 is given to measure which control addresses the specific control objective. The security Analyst can select the control measure rating. It further displays the current risk status for each risk type. It presents the risk events and their calculated risk values, and the control measures that can be used to mitigate the risk. Table 13 displays the new risk status after controls has been implemented.

Table 13. Risk status

Risk Type	Risk Impact Level	Control Measures Implemented			Risk Status
		None	Partial	Full	

Risk Register

A risk register is an important document that provides a tentative record of potential risks in line with vulnerability and threat profile, assets and security goals. The risk register displays the results of the risk calculation. Each risk event is evaluated and presented in a table and the elements used in the calculation, and the calculated risk value. The calculated risk value represents how dangerous the risk event might be for the organisation. The presented risk events are then sorted from the most dangerous to the least dangerous, ensuring that minor risks are not prioritised while more severe risks are overlooked. The risk register displays a table with the list of the risk types, existing control measures and the risk impact level.

REFERENCES

Baldoni, R. (2014). *Critical infrastructure protection: threats, attacks, and countermeasures*. Technical Report. Available online: http://www. dis. uniroma1. it/~ tenace….

Barnum, S. (2008). *Common attack pattern enumeration and classification (capec) schema description.* Http://Capec. Mitre. Org/Documents/Documentation/CAPEC_Schema_DescrIption_v1,3

Barnum, S. (2012). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX). *Mitre Corporation*, *11*, 1–22.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342–353. doi:10.1016/j.technovation.2014.02.001

Canali, D., Bilge, L., & Balzarotti, D. (2014). On the effectiveness of risk prediction based on users browsing behavior. *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, 171–182. 10.1145/2590296.2590347

Castro, J., Kolp, M., & Mylopoulos, J. (2002). Towards requirements-driven information systems engineering: The Tropos project. *Information Systems*, *27*(6), 365–389. doi:10.1016/S0306-4379(02)00012-1

Chen, P. P.-S. (1976). The entity-relationship model—Toward a unified view of data. *ACM Transactions on Database Systems*, *1*(1), 9–36. doi:10.1145/320434.320440

Consortium, W. A. S. (2009). *Web application security consortium threat classification*. Author.

Cord, O. (2001). *Genetic fuzzy systems: evolutionary tuning and learning of fuzzy knowledge bases* (Vol. 19). World Scientific. doi:10.1142/4177

Cordón, O. (2011). A historical review of evolutionary learning methods for Mamdani-type fuzzy rule-based systems: Designing interpretable genetic fuzzy systems. *International Journal of Approximate Reasoning*, *52*(6), 894–913. doi:10.1016/j.ijar.2011.03.004

Dalziell, E. P., & McManus, S. T. (2004). *Resilience, vulnerability, and adaptive capacity: Implications for system performance*. Academic Press.

Dittmeier, C., & Casati, P. (2014). *Evaluating Internal Control Systems: A Comprehensive Assessment Model (CAM) for Enterprise Risk Management*. The Institute of Internal Auditors Research Foundation.

Experian. (2015). *2015 second annual data breach industry forecast*. Author.

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., Blackbird, J., Low, M. K., Mazurek, D., & McKinney, D. (2011). Symantec internet security threat report trends for 2010. *Volume XVI*.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, *30*(1), 28–38. doi:10.1109/MTS.2011.940293

Goodpaster, K. E. (1991). Business ethics and stakeholder analysis. *Business Ethics Quarterly*, *1*(1), 53–73. doi:10.2307/3857592

GOST. (2009). *ISO/IEC 31010-2011 Risk management. Risk assessment methods*. ISO.

HarveyI. (2007). *Introduction To Managing Risk*. Academic Press.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5), e10059. doi:10.2196/10059 PMID:29807882

Kim, K.-D., & Kumar, P. R. (2013). An overview and some challenges in cyber-physical systems. *Journal of the Indian Institute of Science*, *93*(3), 341–352.

Lalonde Levesque, F., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013). A clinical study of risk factors related to malware infections. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 97–108. 10.1145/2508859.2516747

Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M., & Liu, M. (2015). Cloudy with a chance of breach: Forecasting cyber security incidents. *24th USENIX Security Symposium (USENIX Security 15)*, 1009–1024.

Markowski, A. S., & Mannan, M. S. (2009). Fuzzy logic for piping risk assessment (pfLOPA). *Journal of Loss Prevention in the Process Industries*, *22*(6), 921–927. doi:10.1016/j.jlp.2009.06.011

Martin, R. A. (2007). *Common weakness enumeration*. Mitre Corporation.

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. *African Journal of Information and Communication*, *23*(23), 1–26. doi:10.23962/10539/27535

Soska, K., & Christin, N. (2014). Automatically detecting vulnerable websites before they turn malicious. *23rd USENIX Security Symposium (USENIX Security 14)*, 625–640.

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., Whitley, S. M., & Wolf, R. D. (2017). *Finding cyber threats with ATT&CK-based analytics.* The MITRE Corporation, Technical Report No. MTR170202.

Tactic, A. (2017). *Techniques and Common Knowledge*. ATT&CK.

Taylor, J. M., & Sharif, H. R. (2017). Security challenges and methods for protecting critical infrastructure cyber-physical systems. *Selected Topics in Mobile and Wireless Networking (MoWNeT), 2017 International Conference On*, 1–6.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. doi:10.1016/j.cose.2017.09.001

Veeramachaneni, K., Arnaldo, I., Korrapati, V., Bassias, C., & Li, K. (2016). AI^ 2: training a big data machine to defend. *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 49–54.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. doi:10.1016/j.chb.2008.04.005

Wu, W., Kang, R., & Li, Z. (2015). Risk assessment method for cyber security of cyber physical systems. *Reliability Systems Engineering (ICRSE), 2015 First International Conference On*, 1–5.

Yen, T.-F., Heorhiadi, V., Oprea, A., Reiter, M. K., & Juels, A. (2014). An epidemiological study of malware encounters in a large enterprise. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 1117–1130. 10.1145/2660267.2660330

Zadeh, L. A. (1988). Fuzzy logic. *Computer*, *21*(4), 83–93. doi:10.1109/2.53

Zimmermann, H.-J. (2011). *Fuzzy set theory—and its applications*. Springer Science & Business Media.

Chapter 5
PAPR Reduction in OFDM Systems Using Compressive Sensing for Energy-Efficient 5G Networks

Shri Ramtej K.
https://orcid.org/0000-0003-0402-5806
Velagapudi Ramakrishna Siddhartha Engineering College, India

Ramasamy Mariappan
Independent Researcher, India

ABSTRACT

Orthogonal frequency division multiplexing (OFDM) is a multi-carrier transmission technique used to accomplish high data rate transmission in wireless communications. OFDM is one of the major players of multi-carrier communication systems in 5G networks due to its high spectral efficiency and is immune to multipath fading. However, the OFDM signal suffers from significant amplitude fluctuations resulting in a large peak-to-average power ratio (PAPR), which is one of the main downsides of OFDM systems. Therefore, limiting the PAPR in OFDM systems is a key issue, as decreasing PAPR results in lower power consumption and hence an extended battery life. Reducing PAPR without degrading power usage efficiency and bit error rate (BER) is a challenging issue in improving communication performance. This chapter discusses the use of compressive sensing for PAPR reduction in OFDM systems to deploy in energy-efficient 5G networks.

DOI: 10.4018/978-1-6684-3855-8.ch005

INTRODUCTION

To meet the requirements of media-rich wireless services, broadband wireless communications came into existence. But they are subject to multipath frequency selective fading. Also they require complex time domain equalizers which are not practical. Orthogonal frequency division multiplexing (OFDM) is a widely accepted multicarrier communication system in broadband wireless communications owing to its robustness to frequency selective fading channels (Yiyan Wu & Zou, 1995).

The OFDM system is a multicarrier system in which the carrier spacing is wisely chosen such that every sub carrier is orthogonal to other subcarriers. If the dot product of two signals is zero then they are said to be orthogonal to each other. If we multiply two signals and if their integral is zero over an interval, then they are said to be orthogonal in that interval. Orthogonality can be attained by cautiously choosing the sub carrier spacing, for example by choosing the subcarrier spacing which is equal to the multiplicative inverse of the useful symbol period. Since the subcarriers are orthogonal to each other, the spectrum of every subcarrier has a null at the center frequency of each of the other subcarriers in the system. This allows the subcarriers to be spaced as closely as possible without any interference between them. Figure 1(El-Samie et al., 2013) illustrates the block diagram of the OFDM system.

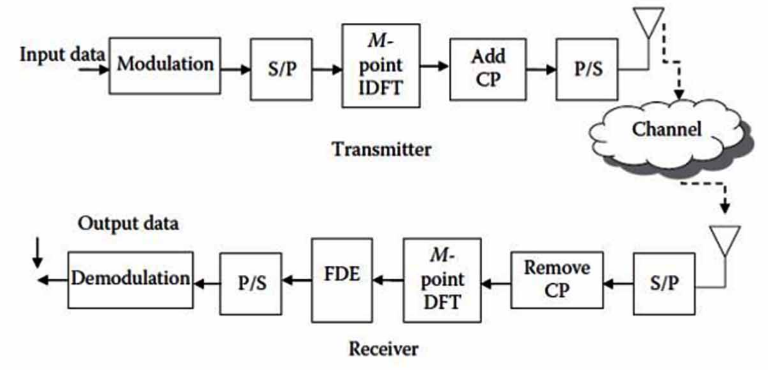
As illustrated in Figure1, the input data symbols are modulated and are serial-to-parallel (S/P) converted and passed through inverse DFT (IDFT) block. Lastly, the cyclic prefix (CP) is appended, and the signal samples are transmitted. The receiver performs the inverse operations of the transmitter. The key advantages of the OFDM system are:

- High spectral efficiency, as orthogonal subcarriers can be overlapped in the frequency domain
- FFT/IFFT operation enables simple digital realization
- Individual subcarriers can use different modulation schemes depending on the transmission conditions on each subcarrier

Because of these advantages, OFDM/OFDMA is being implemented in WiMAX (IEEE 802.16), wireless LAN (IEEE 802.11a and 11g), and third-generation partnership project (3GPP) long term evolution (LTE) downlink systems. Despite these advantages, OFDM system suffers from a large peak to average power ratio (PAPR).

The signal with excessive PAPR generates nonlinear distortion if the power amplifier (PA) does not have highly linear characteristics, and if the input back-off (IBO) is not set properly. If IBO is not set sufficiently, the transmitted signal is corrupted by the nonlinear distortion and causes adjacent channel interference,

Figure 1. Block diagram of the OFDM system



thereby decreasing the system's spectral efficiency. Contrarily, if IBO is increased, the efficiency of PA is reduced, and the heat dissipation is increased. Additionally, a high PAPR requires digital-to-analog (D/A) converters with higher dynamic ranges. The reduction of PAPR leads to PA efficiency improvement, thereby increasing its coverage. Therefore further limiting the PAPR in OFDM systems is a key issue. Decreasing PAPR results in lower power consumption and hence an extended battery life. Reducing PAPR without degrading power usage efficiency and bit error rate (BER) is a challenging issue in improving communication performance.

THE PAPR OF OFDM SIGNALS

To generate OFDM signal inverse DFT and DFT blocks are used at the transmitter side and the receiver side respectively. The symbols are modulated, grouped into blocks of *K* symbols as

$$X = \left[X\left(1\right), X\left(2\right), \ldots, X\left(K\right)\right]^{T}$$

and then passed through an IDFT block. Each symbol $X\left(K\right)$ modulates the k^{th} subcarrier from a set of orthogonal subcarriers. *M*-point IDFT with *L* times oversampling $\left(M = K \times \ell\right)$ is applied on the data block *X*. So, $\left(\ell - 1\right)K$ zeros are padded to the center of baseband symbols. The use of oversampling is to capture all maximum peaks of the continuous OFDM signal. The time-domain OFDM symbols

$$x = \left[x(1), x(2), ..., x(M)\right]^T$$

can be written as

$$x(m) = \frac{1}{\sqrt{M}} \sum_{k=1}^{M} X(k) e^{j2\pi km/M}; \quad m = 1, 2, ..., M \tag{1}$$

As *K* independent modulated subcarriers are added to obtain $x(m)$, this increases PAPR. PAPR is defined as the ratio of maximum power to the average power as given by

$$\text{PAPR} = \frac{\max \left|x(m)\right|^2}{\frac{1}{M} \sum_{m=0}^{M-1} \left|x(m)\right|^2} \tag{2}$$

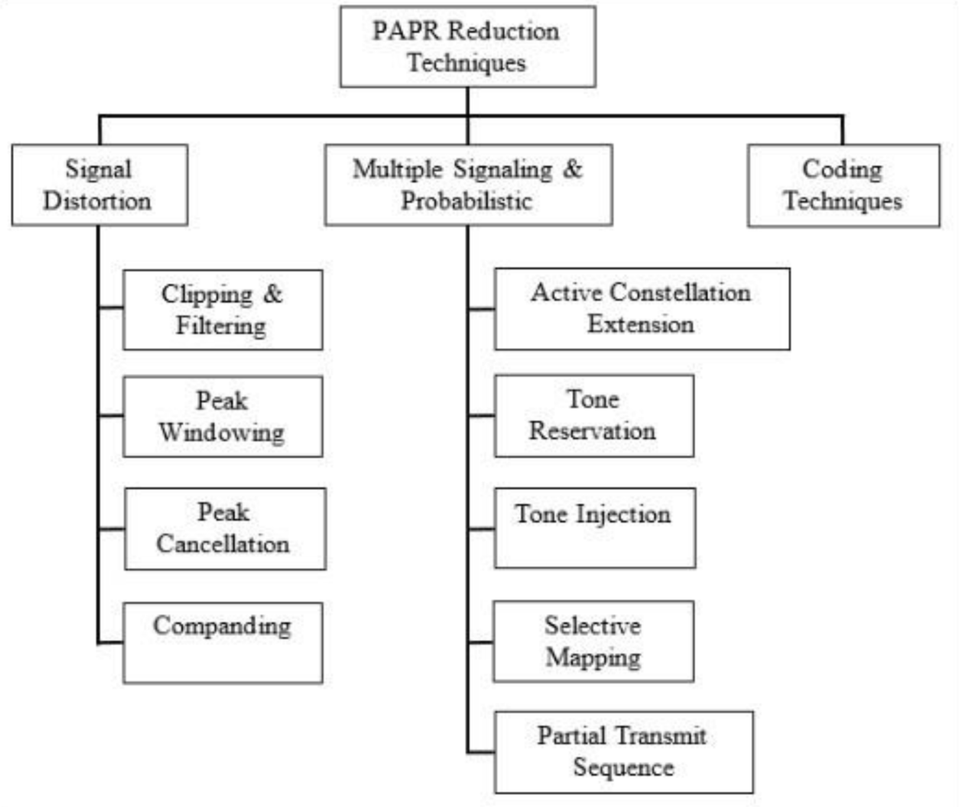
PAPR is a performance measure that designates the power efficiency of the transmitter.

TRADITIONAL PAPR REDUCTION METHODS

Numerous approaches exist in the literature to reduce the PAPR of an OFDM system. These approaches can be mainly divided into three types: signal distortion, multiple signaling and probabilistic techniques, and coding as illustrated in Figure 2 (Jiang & Wu, 2008; Rahmatallah & Mohan, 2013; Seung Hee Han & Jae Hong Lee, 2005). These techniques reduce the PAPR by either clipping, distorting, or adding additional side information to the signal. But, PAPR reduction may also result in BER degradation as there is a change in the nature of modulated signal, which is already at the maximum efficiency achievable (in terms of Euclidean distance between bits). Adding additional side-information reduces the capacity and results in additional energy being added to the signal, thereby degrading the efficiency of the system.

Therefore PAPR reduction techniques may increase BER of the system and might add complexity and cost required for additional signal processing operations. Consequently, the actual advantages of PAPR reduction techniques are found in the systems that can reduce PAPR without a significant effect on BER performance and avoids additional system complexity. Hence there is a trade-off among PAPR reduction, BER degradation, and system complexity.

Figure 2. Classification of PAPR reduction techniques



Clipping and Filtering

Clipping is the simplest signal distortion based PAPR reduction method. In this technique, the signal peaks of $x(m)$ are clipped when the peak values exceed a specific threshold, α_0 as described by

$$x_c(m) = \begin{cases} x(m), \left|x(m)\right| \le \alpha_0 \\ \alpha_0 e^{j\phi(m)}, \left|x(m)\right| > \alpha_0 \end{cases} \tag{3}$$

where $\phi(m)$ is the phase of $x(m)$. This is a straightforward PAPR reduction method, as no side information is necessary to transmit to the receiver. Nevertheless, clipping introduces both in-band and out-of-band distortions (Ochiai & Imai, n.d.). Therefore, it is essential to filter the clipped signal to reduce out-of-band distortions. But filtering cannot reduce in-band distortions, which causes BER degradation (Ochiai & Imai, 2002). But, oversampling can decrease the effect of in-band distortions as some part of the noise is reshaped out of the signal band, which can be eliminated by filtering operation (Saeedi et al., 2002). Filtering the clipped signal can maintain spectral efficiency by removing the out-of-band radiations, thereby improving the performance of BER. However, it causes peak power regrowth. Various iterative clipping and filtering (Armstrong, 2002; Hangjun Chen & Haimovich, 2003; O'Neill & Lopes, n.d.; Xiaodong Li & Cimini, 1998) techniques have been proposed to minimize the overall peak power regrowth.

Peak Windowing

Peak windowing reduces higher peaks by multiplying them with a weighting function known as window function (G. Chen et al., 2009; van Nee & de Wild, n.d.), in contrast to peak clipping, where the peaks that exceed a predefined threshold are hard-limited. Various window functions with good spectral properties can be used in this process. Hanning, Hamming, and Kaiser windows are the most commonly used window functions. To diminish PAPR, a window function is aligned with the signal samples in such a fashion that its higher amplitudes are multiplied by lower amplitude signal samples, and its lower amplitudes are multiplied by the signal peaks. Hence, the signal peaks are attenuated more smoothly in contrast to the hard clipping, thereby causing reduced distortion.

Peak Cancellation

Here a peak cancellation signal is adequately generated, scaled, shifted, and subtracted from the OFDM signal at the segments which exhibit higher peaks. Now the generated waveform is band limited to specific peak cancellation tones that are not used for transmission (Jeon et al., 2012; Song & Ochiai, 2016). In the OFDM transmitter after the IDFT block, a peak detector is used to detect the peaks higher than a specific threshold. Then a peak cancellation sognal is generated and subtracted from the OFDM signal. Peak cancellation process should be performed carefully so that new peaks are not generated.

Companding

Companding techniques are normally used to optimize the required number of bits per sample in speech signals. As speech signals and OFDM signals have a similar structure i.e., high peaks occur occasionally, these companding techniques can be employed to decrease the PAPR of OFDM signal (Huang et al., 2001; Xiao Huang et al., n.d.). Companding transforms have comparatively low computational complexity in comparison to other methods, and their complexity is not influenced by the number of subcarriers. Moreover, they do not require the transmission of side information and, therefore, doesn't decrease the bit rate. Due to their implementation simplicity and the benefits they provide, companding techniques became an attractive method to reduce PAPR. However, the PAPR reduction achieved by companding techniques comes with the cost of an increase in BER.

The application of the μ-law companding to decrease PAPR is investigated in (Pratt et al., 2006; Wang et al., 1999; Xianbin Wang et al., 1999). μ-law companding enhances the lower amplitudes while maintaining the high peaks of the signal. Hence the peak power is unaltered, and average power is increased, thereby reducing the PAPR. To accommodate this increase in average power, the gain of power amplifier should be adjusted dynamically, which increases the hardware cost. The authors in (Wang et al., 1999) investigated the impact of companding on the OFDM system's BER performance in the presence of AWGN channel and demonstrated that a reasonable symbol error rate could be obtained by appropriately selecting the companding parameters.

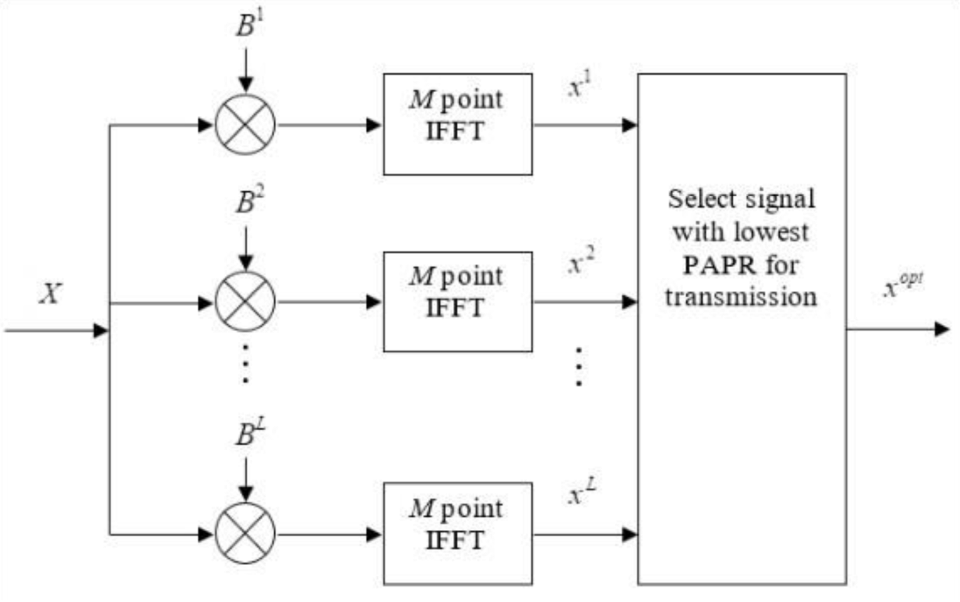
Coding Techniques

The coding techniques that offer error detection and correction can be modified to perform PAPR reduction with a tolerable extra complexity. One of the popular techniques for decreasing PAPR is block coding (Wilkinson et al., 1994). In this method, input data is encoded to a codeword where some bits are dedicated to decreasing PAPR instead of enhancing BER. For instance, to decrease the PAPR of a signal with 4 subcarriers, 3-bit input data can be mapped to a 4-bit codeword by adding a parity bit. By optimizing the position of the parity bit, PAPR can be reduced further. Moreover, by dividing the lengthy information sequences into sub-blocks and by employing different coding techniques to encode each sub-block (Zhang et al., n.d.), PAPR can be reduced by optimizing their combination. But the information of the coding techniques used and the location of parity bits should be transmitted to the receiver as side information.

Active Constellation Extension (ACE)

The ACE technique for PAPR reduction in OFDM is well reported in (He & Yan, 2013; Kang et al., 2007; Brian Scott Krongold & Jones, 2003; Prabhu & Grayver, 2009; Z. Yang et al., 2005; Zhou & Jiang, 2009). It is an effective technique to decrease the PAPR without the need for side information transmission. The projection-onto-convex-sets (POCS) algorithm of the ACE technique clips the time domain signal

Figure 3. Constellation map describing the allowable extension region for ACE considering QPSK modulation



and extends the outer constellation points out of the original constellation without decreasing the minimum Euclidean distance.

The fundamental principle of ACE techniques for PAPR reduction is described in Figure3. The constellation points may be extended into areas representing gray regions during the reconstruction phase after clipping the time domain signal. PAPR can be reduced by extending the constellations into these regions at the cost of a small increment in average power. This increment degrades the system's BER performance. But this degradation is somewhat compensated as the gray regions result in an increase in the minimum Euclidean distance. So there is a fair trade-off between the PAPR reduction and BER degradation (Brian Scott Krongold & Jones, 2003). Also, this method increases the average power of the transmitted signal and has a limitation when applied to modulation schemes with larger constellation sizes (Seung Hee Han & Jae Hong Lee, 2005).

Tone Reservation (TR)

TR is a method that uses reserved subcarriers to decrease the PAPR of a signal (J.-C. Chen et al., 2011; Dae-Woon Lim et al., 2009; B.S. Krongold & Jones, 2004; H. Li et al., 2011; Luqing Wang & Tellambura, 2008; Zabre et al., 2006). Similar to the

ACE technique, pre-transmission clipping, and constellation reconstruction are used to reduce the PAPR of a time-domain signal. Nevertheless, the main difference is in the utilization of reserved tones in place of distorted constellations. In this method, a time-domain vector x is added to the OFDM signal to modify its statistical distribution that helps in reducing PAPR. The tricky thing now is to determine x that reduces the maximum peak value of the new OFDM signal. The amount of PAPR reduction in this method depends on the number of reserved subcarriers, their locations, and the optimization complexity. The locations of these reserved subcarriers should be transmitted as side information to the receiver. If the number of subcarriers is small in OFDM systems, these reserved subcarriers might decrease the data rate. Standard TR has the disadvantage of a slow convergence time as that of POCS ACE (B.S. Krongold & Jones, 2004). Gradient projection method is suggested to be used in (B.S. Krongold & Jones, 2004) similar to that of Smart Gradient Projection (SGP) ACE to converge quickly.

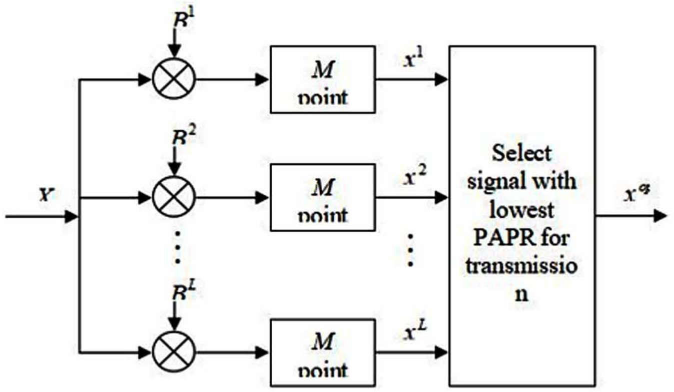
Tone Injection (TI)

Tellado has introduced TI to overcome the data rate loss problem in TR (J.-C. Chen & Wen, 2010; J. Tellado, 1999; J. Tellado and J. M. Cioffi, 1998; S. H. Han et al., 2006). The central idea is to expand the constellation size so that each point in the original constellation is mapped onto various other points in the expanded constellation before IDFT processing. Considering a square QAM constellation with size M and spacing of d between the original points, the minimum distance between each point in the original constellation and its equivalent points in the expanded constellation should be $D = d\sqrt{M}$ (Rahmatallah & Mohan, 2013) to maintain the BER performance. TI doesn't require any side information transmission, and so there is no loss of bit rate. Despite its benefits, TI increases the complexity of the transmitter. Also, it increases average signal power due to the expansion of the signal constellation. TI offers two degrees of freedom, one being the selection of tones and other being the expanded constellation's size. Discovering the right possible combination requires high complexity.

Selective Mapping (SLM)

SLM is a simple method where L different OFDM signals are generated, which represent the original data, and the signal with the least PAPR is transmitted (Bäuml et al., 1996; Breiling et al., 2001; Chin-Liang Wang & Yuan Ouyang, 2005; S.H. Han & Lee, 2004; C. P. Li et al., 2010; Yung-Lyul Lee et al., 2003). This is accomplished

Figure 4. SLM technique for OFDM



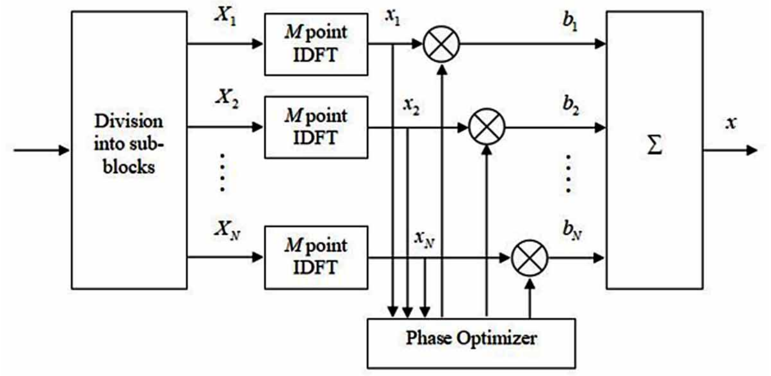
by generating a set of L distinct phase rotated vectors and multiplying them with the original subcarriers, as depicted in Figure 4.

This method utilizes the independence of various phase rotated subcarriers and hence ensuring time-domain signals with distinct PAPR values (Bäuml et al., 1996). To decrease the complexity, phase rotation vectors are usually considered as multiples of $\pi / 2$. The amount of reduction in PAPR depends on the number of phase sequences generated and their design. The complexity increases due to the need for L modulators to generate L different time-domain signals. Another disadvantage is the requirement of side information of $\lfloor \log_2 L \rfloor$ bits to inform the receiver which sequence was selected for transmission. As this side information is crucial for accurate demodulation, it requires an additional level of coding, to protect it from corruption. SLM technique, which doesn't require side information, is proposed in (Breiling et al., 2001). But, this method comes with the price of additional complexity in the form of scramblers with a little redundancy introduced. If side information is protected by channel coding, no side information is required. At the receiver side, L decoders process the received signal using L possible phase rotated vectors to recover the data (Bäuml et al., 1996). But often, there are space limitations at the receiver side, particularly in the case of mobile devices.

Partial Transmit Sequence (PTS)

In this method, the input data block is partitioned into N disjoint frames. Then all the frames are weighted by different optimal phase factors and added so that the combined signal has a lower PAPR (Alavi et al., 2005; Seung Hee Han & Lee, 2004; Müller & Huber, 1997; L. Yang et al., 2006), as shown in Figure 5. The complexity

Figure 5. PTS technique for OFDM



of the PTS technique is high, as the selection of the optimal phase rotation factor requires an exhaustive search. Also, PTS requires additional N-1 IDFT blocks and side information transmission to demodulate the data-carrying subcarriers perfectly.

PAPR reduction capability can be enhanced by increasing the number of possible phase rotation factors W and the number of disjointed frames N. But the complexity of the search algorithm grows exponentially with N (Seung Hee Han & Jae Hong Lee, 2005). So, the complexity is of the form $O\left(W^N\right)$ and to overcome the search complexity, techniques commonly employ only 2 $\left\{\pm 1\right\}$ or 4 $\left\{\pm 1, \pm j\right\}$ possible rotation factors and restrict the number of disjoint frames to 4. Several techniques are proposed to decrease the computational complexity of PTS technique. In (Müller & Huber, 1997), a threshold is used to avoid undesirable search, once the required PAPR performance is attained. In (L. Yang et al., 2006) a smart search algorithm is employed to decrease the complexity of the search algorithm for optimal phase factors.

COMPRESSIVE SENSING

Compressive sensing (CS), also known as compressive sampling is a novel sensing/sampling example that goes contrary to the common wisdom in data acquisition. CS theory affirms that certain signals and images can be recovered from far fewer samples or measurements than required by traditional methods. CS relies on two principles to make this possible: sparsity, which pertains to the signals of interest, and incoherence, which pertains to the sensing modality (Candes & Wakin, 2008).

Sparsity expresses the idea that the "information rate" of a continuous time signal can be much lesser than suggested by its bandwidth, or that a discrete-time signal depends on a number of degrees of freedom which is comparably much smaller than its (finite) length. CS exploits the fact that many natural signals are sparse or compressible i.e. they can be represented concisely when expressed in the proper basis Ψ. Incoherence extends the duality between time and frequency and expresses the idea that objects having a sparse representation in Ψ must be spread out in the domain in which they are acquired, just as a Dirac in the time domain is spread out in the frequency domain. In other words, incoherence says that unlike the signal of interest, the sampling or sensing waveforms have an extremely dense representation in Ψ.

The main idea is that one can design effective sensing or sampling protocols that capture the useful information content embedded in a sparse signal and compress it into a small amount of data. These protocols are non-adaptive and simply require correlating the signal with a small number of fixed waveforms that are incoherent with the sparsifying basis. The most remarkable thing about these sampling protocols is that they allow a sensor to capture the information efficiently in a sparse signal without trying to comprehend that signal. Further, there is a way to use numerical optimization to reconstruct the full-length signal from the small amount of collected data. In other words, CS is a very simple and efficient signal acquisition protocol, which samples in a signal independent fashion at a low rate and later uses computational power for reconstruction from what appears to be an incomplete set of measurements.

Compressive Sensing for PAPR Reduction

In CS, desired sparse signal $X^s \in C^M$ is recovered from noisy measured information $y \in C^N$ which is linearly obtained by (Azarnia et al., 2020)

$$y = G\Psi X^s + e = \Phi X^s + e \tag{4}$$

where $G \in R^{N\times M}$ is a mapping matrix and its elements are Gaussian random variables with zero mean and unit variance, $\Psi \in C^{M\times M}$ is the IDFT matrix, $X^s \in C^M$ is a sparse vector, $\Phi = G\Psi$, and $e \in C^N$ is the measurement error. Usually, the number of measurements *N* is smaller than the signal length *M*. The time-domain OFDM symbols $x = \Psi X^s$ is compressed by the matrix G.

Different Gaussian matrices $G_i (i = 1, 2, ..., I)$ are constructed to generate several signals. Amongst them the signal with the lowest PAPR is selected for transmission.

The amount of PAPR reduction depends on the number of candidate matrices *I*. The orthogonalization of the matrix G leads to the accurate detection of the original symbols. Gram–Schmidt technique is used to orthogonalize the Gaussian matrix to avoid degradation in BER performance. During the procedure of the Gram–Schmidt, the columns of matrix $G(g_1, g_2, ..., g_M)$ are replaced with the new orthogonal columns $\hat{g}_1, \hat{g}_2, ..., \hat{g}_M$ as

$$\hat{g}_1 = \frac{g_1}{\left\| g_1 \right\|} \tag{5}$$

For $u = 2, 3, ., . M$, we have

$$\hat{g}_u = \frac{g_u - \sum_{i=1}^{u-1} (g_u, \hat{g}_i)\hat{g}_i}{\left\| g_u - \sum_{i=1}^{u-1} (g_u, \hat{g}_i)\hat{g}_i \right\|} \tag{6}$$

Before transmitting the data, Gaussian matrices are generated, orthogonalized, and stored in the transmitter and receiver. The order of the matrix which produced the lowest PAPR is sent as side information. Therefore, only $\log_2 I$ bits are needed to send the side information.

In this technique, the DFT operation at the receiver side is not required because of the universality of the CS theory. The sparsity does not often happen to the canonical basis, rather than occurs to another orthonormal basis. The signal is not sparse in the time-domain but is sparse in the DFT domain because of oversampling. As the CS results in the DFT-domain signal directly, it is not needed to multiply it with the DFT matrix. As $y = G\Psi X^s + e$ is the vector of interest, reconstructing X^s from y is equivalent to reconstructing X^s from $\Phi X^s + e$.

The orthogonal matching pursuit (OMP) algorithm is the most widely used greedy algorithm for PAPR reduction due to its simplicity. Like other CS techniques, this technique will be strong when the mapping matrix fulfills the restricted isometry property (RIP). One significant achievement of CS theory is that certain classes of randomly generated matrices called Gaussian and Bernoulli matrices provide the RIP with very high probability.

FILTERED OFDM FOR 5G NETWORKS

The filtered orthogonal frequency division multiplexing (F-OFDM) framework has been suggested as a waveform contender for 5G communication networks. The F-OFDM has salient features such as convenient design, support for symmetrical transmission and PAPR reduction procedures, improved spectral efficiency, support for multi- antenna transmission strategies like the OFDM framework, low computational complexity, suppression of OOBE level, low latency and support for asynchronous transmission. Be that as it may, the high PAPR esteem keeps on being the primary issue of the F-OFDM waveform candidate, since this framework upholds symmetrical transmission. The additional filter is the fundamental driver for the increase of PAPR value of the F-OFDM candidate. This is on the grounds that the filter bank makes the power circulation among the examples be more extensive than that in the OFDM framework, which brings about a reduction in the mean power of the sign and subsequently debasement in the HPA proficiency at the transmitter. Nonetheless, the F-OFDM framework upholds the PAPR reduction techniques. Consequently, selective mapping, partial transmit sequence, and the interleaving technique can be utilized to diminish the high PAPR values of F-OFDM.

In the current literature, several investigations and experiments were performed to increase the spectral efficiency of OFDM to fulfill the necessities of 5G applications. The concealment of out-of-band discharge (OOBE) and offbeat transmission are the unmistakable highlights of the filtering based waveform structures. In the meantime, the high peak-to-average power ratio (PAPR) is as yet difficult for the new waveform types. Partial transmit sequence is a powerful procedure for relieving the pattern of high PAPR in multicarrier frameworks for 5G communication networks. In the current literature the PTS procedure is utilized to diminish the high PAPR worth of a F-OFDM framework. Then, at that point, this framework is contrasted and the OFDM framework. Moreover, the other related boundaries, for example, frequency localization, bit error rate (BER), and computational complexity are assessed and investigated for the two frameworks with and without PTS. The F-OFDM using PTS accomplishes more elevated levels of PAPR, BER, and OOBE performances, compared to OFDM. Besides, the BER performance of F-OFDM is not influenced by the utilization of the PTS method.

FUTURE RESEARCH DIRECTIONS

There are many improved versions of orthogonal matching pursuit (OMP), like Regularized OMP (Deanna Needell & Vershynin, 2009), Stagewise OMP (Donoho et al., 2012), Compressive Sampling Matching Pursuits (CoSaMP) (D. Needell & Tropp, 2009), Subspace Pursuits (Dai & Milenkovic, 2009), Gradient Pursuits (Figueiredo et al., 2007) and Orthogonal Multiple Matching Pursuit (Liu & Temlyakov, 2012). The performance of these techniques can be studied and used in OFDM and F-OFDM system to recover the original signal depending on their complexity.

The 5G communication network has many challenges such as high data rates and spectral efficiency, etc. One solution may be utilizing multicarrier modulations (MCMs). Nonetheless, utilizing MCMs is inseparable from low energy efficiency because of their high PAPR. Without a doubt, high PAPR signals drive power speakers to work more often than not in the direct zone. This last option relates to low power efficiency. This prompts a compromise among spectral efficiency and energy proficiency. Hence, there is a need of an optimal method to solve this trade off.

The next generation communication networks are relied upon to give a lot higher information throughput and dependable associations for a far bigger number of remote assistance endorsers and machine-type hubs, which brings about progressively severe necessities of spectral efficiency (SE) and energy efficiency (EE). OFDM with index modulation (OFDM-IM) stands apart as a promising answer for fulfill the SE prerequisite with a sensible expansion in framework intricacy. In any case, the EE of OFDM-IM is as yet needed to be improved. In addition, variety gain is hard to collect from the recurrence space without influencing the SE for OFDM-IM frameworks, which blocks further unwavering quality upgrade. Hence, a lot of research is needed to improve spectral efficiency of OFDM-IM without compromising the quality.

CONCLUSION

This chapter describes PAPR in OFDM system, problems associated with high PAPR, and the various PAPR reduction techniques that have been used in the literature. The application of compressive sensing for PAPR reduction in OFDM system has been discussed. In this technique, the time-domain OFDM signal generated after the inverse DFT will be compressed at the transmitter side using a Gaussian random matrix. At the receiver side, orthogonal matching pursuit (OMP) reconstruction algorithm can be used to recover the original OFDM symbols. Other improved versions of OMP can be exploited to improve the performance of the system. These techniques can also be applied to F-OFDM as it has been suggested as a waveform contender for 5G communication networks.

REFERENCES

Alavi, A., Tellambura, C., & Fair, I. (2005). PAPR reduction of OFDM signals using partial transmit sequence: An optimal approach using sphere decoding. *IEEE Communications Letters*, *9*(11), 982–984. doi:10.1109/LCOMM.2005.11014

Armstrong, J. (2002). Peak-to-average power reduction for OFDM by repeated clipping and frequency domain filtering. *Electronics Letters*, *38*(5), 246. doi:10.1049/el:20020175

Azarnia, G., Sharifi, A. A., & Emami, H. (2020). Compressive sensing based PAPR reduction in OFDM systems: Modified orthogonal matching pursuit approach. *ICT Express*, *6*(4), 368–371. doi:10.1016/j.icte.2020.07.004

Bäuml, R. W., Fischer, R. F. H., & Huber, J. B. (1996). Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping. *Electronics Letters*, *32*(22), 2056. doi:10.1049/el:19961384

Breiling, H., Muller-Weinfurtner, S. H., & Huber, J. B. (2001). SLM peak-power reduction without explicit side information. *IEEE Communications Letters*, *5*(6), 239–241. doi:10.1109/4234.929598

Candes, E. J., & Wakin, M. B. (2008). An Introduction To Compressive Sampling. *IEEE Signal Processing Magazine*, *25*(2), 21–30. doi:10.1109/MSP.2007.914731

Chen, G., Ansari, R., & Yao, Y. (2009). Improved peak windowing for PAPR reduction in OFDM. *IEEE Vehicular Technology Conference*, 4–8. 10.1109/VETECS.2009.5073593

Chen, H., & Haimovich, A. M. (2003). Iterative estimation and cancellation of clipping noise for OFDM signals. *IEEE Communications Letters*, *7*(7), 305–307. doi:10.1109/LCOMM.2003.814720

Chen, J.-C., Chiu, M.-H., Yang, Y.-S., & Li, C.-P. (2011). A Suboptimal Tone Reservation Algorithm Based on Cross-Entropy Method for PAPR Reduction in OFDM Systems. *IEEE Transactions on Broadcasting*, *57*(3), 752–756. doi:10.1109/TBC.2011.2127590

Chen, J.-C., & Wen, C.-K. (2010). PAPR Reduction of OFDM Signals Using Cross-Entropy-Based Tone Injection Schemes. *IEEE Signal Processing Letters*, *17*(8), 727–730. doi:10.1109/LSP.2010.2051617

Dai, W., & Milenkovic, O. (2009). Subspace Pursuit for Compressive Sensing Signal Reconstruction. *IEEE Transactions on Information Theory*, *55*(5), 2230–2249. doi:10.1109/TIT.2009.2016006

Donoho, D. L., Tsaig, Y., Drori, I., & Starck, J.-L. (2012). Sparse Solution of Underdetermined Systems of Linear Equations by Stagewise Orthogonal Matching Pursuit. *IEEE Transactions on Information Theory*, *58*(2), 1094–1121. doi:10.1109/TIT.2011.2173241

El-Samie, F., Al-kamali, F., Al-nahari, A., & Dessouky, M. (2013). *SC-FDMA for Mobile Communications*. CRC Press. doi:10.1201/b15157

Figueiredo, M., Nowak, R. D., & Wright, S. J. (2007). Gradient Projection for Sparse Reconstruction: Application to Compressed Sensing and Other Inverse Problems. *IEEE Journal of Selected Topics in Signal Processing*, *1*(4), 586–597. doi:10.1109/JSTSP.2007.910281

Han, S. H., Cioffi, J. M., & Lee, J. H. (2006). Tone injection with hexagonal constellation for peak-to-average power ratio reduction in OFDM. *IEEE Communications Letters*, *10*(9), 646–648. doi:10.1109/LCOMM.2006.1714532

Han, S. H., & Lee, J. H. (2004). Modified Selected Mapping Technique for PAPR Reduction of Coded OFDM Signal. *IEEE Transactions on Broadcasting*, *50*(3), 335–341. doi:10.1109/TBC.2004.834200

Han, S. H., & Lee, J. H. (2004). PAPR reduction of OFDM signals using a reduced complexity PTS technique. *IEEE Signal Processing Letters*, *11*(11), 887–890. doi:10.1109/LSP.2004.833490

Han, S. H., & Lee, J. H. (2005). An overview of peak-to-average power ratio reduction techniques for multicarrier transmission. *IEEE Wireless Communications*, *12*(2), 56–65. doi:10.1109/MWC.2005.1421929

He, J., & Yan, Z. (2013). Improving convergence rate of active constellation extension algorithm for PAPR reduction in OFDM. *2013 IEEE International Conference on Information and Automation (ICIA)*, 280–284. 10.1109/ICInfA.2013.6720310

Huang, X., & Lu, J. (n.d.). Companding transform for the reduction of peak-to-average power ratio of OFDM signals. *IEEE VTS 53rd Vehicular Technology Conference, Spring 2001. Proceedings, 2*, 835–839. 10.1109/VETECS.2001.944496

Huang, X., Lu, J., Zheng, J., Chuang, J., & Gu, J. (2001). Reduction of peak-to-average power ratio of OFDM signals with companding transform. *Electronics Letters*, *37*(8), 506. doi:10.1049/el:20010345

Jeon, H.-B., No, J.-S., & Shin, D.-J. (2012). A New PAPR Reduction Scheme Using Efficient Peak Cancellation for OFDM Systems. *IEEE Transactions on Broadcasting*, *58*(4), 619–628. doi:10.1109/TBC.2012.2211432

Jiang, T., & Wu, Y. (2008). An overview: Peak-to-average power ratio reduction techniques for OFDM signals. *Broadcasting. IEEE Transactions On*, *54*(2), 257–268. doi:10.1109/TBC.2008.915770

Kang, B. M., Ryu, H.-G., & Ryu, S. B. (2007). A PAPR Reduction Method using New ACE (Active Constellation Extension) with Higher Level Constellation. *2007 IEEE International Conference on Signal Processing and Communications*, 724–727. 10.1109/ICSPC.2007.4728421

Krongold, B. S., & Jones, D. L. (2003). PAR reduction in OFDM via active constellation extension. *IEEE Transactions on Broadcasting*, *49*(3), 258–268. doi:10.1109/TBC.2003.817088

Krongold, B. S., & Jones, D. L. (2004). An Active-Set Approach for OFDM PAR Reduction via Tone Reservation. *IEEE Transactions on Signal Processing*, *52*(2), 495–509. doi:10.1109/TSP.2003.821110

Lee, Y.-L., You, Y.-H., Jeon, W.-G., Paik, J.-H., & Song, H.-K. (2003). Peak-to-average power ratio in MIMO-OFDM systems using selective mapping. *IEEE Communications Letters*, *7*(12), 575–577. doi:10.1109/LCOMM.2003.821329

Li, C. P., Wang, S. H., & Wang, C. L. (2010). Novel low-complexity SLM schemes for PAPR reduction in OFDM systems. *IEEE Transactions on Signal Processing*, *58*(5), 2916–2921. doi:10.1109/TSP.2010.2043142

Li, H., Jiang, T., & Zhou, Y. (2011). An Improved Tone Reservation Scheme With Fast Convergence for PAPR Reduction in OFDM Systems. *IEEE Transactions on Broadcasting*, *57*(4), 902–906. doi:10.1109/TBC.2011.2169622

Li, X., & Cimini, L. J. (1998). Effects of clipping and filtering on the performance of OFDM. *IEEE Communications Letters*, *2*(5), 131–133. doi:10.1109/4234.673657

Lim, D.-W., Noh, H.-S., Jeon, H.-B., No, J.-S., & Shin, D.-J. (2009). Multi-Stage TR Scheme for PAPR Reduction in OFDM Signals. *IEEE Transactions on Broadcasting*, *55*(2), 300–304. doi:10.1109/TBC.2009.2013988

Liu, E., & Temlyakov, V. N. (2012). The Orthogonal Super Greedy Algorithm and Applications in Compressed Sensing. *IEEE Transactions on Information Theory*, *58*(4), 2040–2047. doi:10.1109/TIT.2011.2177632

Müller, S. H., & Huber, J. B. (1997). OFDM with reduced peak-to-average power ratio by optimum combination of partial transmit sequences. *Electronics Letters*, *33*(5), 368. doi:10.1049/el:19970266

Needell, D., & Tropp, J. A. (2009). CoSaMP: Iterative signal recovery from incomplete and inaccurate samples. *Applied and Computational Harmonic Analysis*, *26*(3), 301–321. doi:10.1016/j.acha.2008.07.002

Needell, D., & Vershynin, R. (2009). Uniform Uncertainty Principle and Signal Recovery via Regularized Orthogonal Matching Pursuit. *Foundations of Computational Mathematics*, *9*(3), 317–334. doi:10.100710208-008-9031-3

O'Neill, R., & Lopes, L. B. (n.d.). Envelope variations and spectral splatter in clipped multicarrier signals. *Proceedings of 6th International Symposium on Personal, Indoor and Mobile Radio Communications*, *1*, 71–75. 10.1109/PIMRC.1995.476406

Ochiai, H., & Imai, H. (2002). Performance analysis of deliberately clipped OFDM signals. *IEEE Transactions on Communications*, *50*(1), 89–101. doi:10.1109/26.975762

Ochiai, H., & Imai, H. (n.d.). On clipping for peak power reduction of OFDM signals. *Globecom '00 - IEEE. Global Telecommunications Conference. Conference Record, 2*, 731–735. 10.1109/GLOCOM.2000.891236

Prabhu, R. S., & Grayver, E. (2009). Active constellation modification techniques for OFDM PAR reduction. *2009 IEEE Aerospace Conference*, 1–8. 10.1109/AERO.2009.4839406

Pratt, T. G., Jones, N., Smee, L., & Torrey, M. (2006). OFDM Link Performance With Companding for PAPR Reduction in the Presence of Non-Linear Amplification. *IEEE Transactions on Broadcasting*, *52*(2), 261–267. doi:10.1109/TBC.2006.875613

Rahmatallah, Y., & Mohan, S. (2013). Peak-to-average power ratio reduction in ofdm systems: A survey and taxonomy. *IEEE Communications Surveys and Tutorials*, *15*(4), 1567–1592. doi:10.1109/SURV.2013.021313.00164

Saeedi, H., Sharif, M., & Marvasti, F. (2002). Clipping noise cancellation in OFDM systems using oversampled signal reconstruction. *IEEE Communications Letters*, *6*(2), 73–75. doi:10.1109/4234.984699

Song, J., & Ochiai, H. (2016). Performance Analysis for OFDM Signals With Peak Cancellation. *IEEE Transactions on Communications*, *64*(1), 261–270. doi:10.1109/TCOMM.2015.2502585

Tellado, J. (1999). *Peak to Average Ratio Reduction for Multi-carrier Modulation* [PhD Thesis]. Stanford University, Stanford, CA, USA.

Tellado, J., & Cioffi, J. M. (1998). Peak power reduction for multicarrier transmission. *Proc. IEEE Global Communications Conference (CLOBECOM).*

van Nee, R., & de Wild, A. (n.d.). Reducing the peak-to-average power ratio of OFDM. *VTC '98. 48th IEEE Vehicular Technology Conference. Pathway to Global Wireless Revolution, 3*, 2072–2076. 10.1109/VETEC.1998.686121

Wang, C.-L., & Yuan, O. (2005). Low-complexity selected mapping schemes for peak-to-average power ratio reduction in OFDM systems. *IEEE Transactions on Signal Processing*, *53*(12), 4652–4660. doi:10.1109/TSP.2005.859327

Wang, L., & Tellambura, C. (2008). Analysis of Clipping Noise and Tone-Reservation Algorithms for Peak Reduction in OFDM Systems. *IEEE Transactions on Vehicular Technology*, *57*(3), 1675–1694. doi:10.1109/TVT.2007.907282

Wang, X., Tjhung, T. T., & Ng, C. S. (1999). Reduction of peak-to-average power ratio of OFDM system using a companding technique. *IEEE Transactions on Broadcasting*, *45*(3), 303–307. doi:10.1109/11.796272

Wang, X., Tjhung, T. T., & Ng, C. S. (1999). Reply to the comments on "Reduction of peak-to-average power ratio of OFDM system using a companding technique." *IEEE Transactions on Broadcasting*, *45*(4), 420–422. doi:10.1109/11.825538

Wilkinson, T. A., Jones, A. E., & Barton, S. K. (1994). Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes. *Electronics Letters*, *30*(25), 2098–2099. doi:10.1049/el:19941423

Wu, Y., & Zou, W. Y. (1995). Orthogonal frequency division multiplexing: A multicarrier modulation scheme. *IEEE Transactions on Consumer Electronics*, *41*(3), 392–399. doi:10.1109/30.468055

Yang, L., Chen, R. S., Siu, Y. M., & Soo, K. K. (2006). PAPR Reduction of an OFDM Signal by Use of PTS With Low Computational Complexity. *IEEE Transactions on Broadcasting*, *52*(1), 83–86. doi:10.1109/TBC.2005.856727

Yang, Z., Fang, H., & Pan, C. (2005). ACE With Frame Interleaving Scheme to Reduce Peak-to-Average Power Ratio in OFDM Systems. *IEEE Transactions on Broadcasting*, *51*(4), 571–575. doi:10.1109/TBC.2005.851697

Zabre, S., Palicot, J., Louet, Y., & Lereau, C. (2006). SOCP Approach for OFDM Peak-to-Average Power Ratio Reduction in the Signal Adding Context. *2006 IEEE International Symposium on Signal Processing and Information Technology*, 834–839. 10.1109/ISSPIT.2006.270914

Zhang, Y., Yongacoglu, A., Chouinard, J.-Y., & Zhang, L. (n.d.). OFDM peak power reduction by sub-block-coding and its extended versions. *1999 IEEE 49th Vehicular Technology Conference, 1*, 695–699. 10.1109/VETEC.1999.778254

Zhou, Y., & Jiang, T. (2009). A novel clipping integrated into ACE for PAPR reduction in OFDM systems. *2009 International Conference on Wireless Communications & Signal Processing*, 1–4. 10.1109/WCSP.2009.5371552

Chapter 6
Prediction of Ethereum Blockchain ERC-20 Token Standard Smart Contract Vulnerabilities Using Source Code Metrics:
An Ensemble Learning Approach

Nemitari Ajienka
Nottingham Trent University, UK

Richard Ikechukwu Otuka
Nottingham Trent University, UK

ABSTRACT

In this study, firstly, a dataset of 10,476 annotated vulnerable ERC-20 standard token smart contracts (belonging to a set of 33 common smart contract vulnerabilities) has been collected from a publicly available repository. Secondly, using the SolMet smart contract metrics measurement tool, the object-oriented software attributes (i.e., metrics) from each smart contract's source code has been extracted. Lastly, using the source code metrics and the vulnerability annotations (i.e., labels) as the input in supervised machine learning (classification) algorithms, the accuracy of each individual algorithm is evaluated against the accuracy of an ensemble classifier (namely voting). The model accuracies demonstrate the feasibility of identifying and prioritising smart contracts for further inspection prior to deployment to the blockchain network. The ensemble classifier performed better (accuracy = 0.79) compared to each classifier when used individually.

DOI: 10.4018/978-1-6684-3855-8.ch006

INTRODUCTION

Ethereum can be viewed as a huge transaction-based state machine, where its state is updated after every transaction. A Smart Contract (SC) is a program deployed and stored in the Ethereum blockchain by a contract-creation transaction. Given the immutable nature of the blockchain, once a SC has been deployed it cannot be modified or updated. In addition, many identified bugs and vulnerabilities in smart contracts have led to significant financial losses (e.g., $50 million the case of the DAO hack), which raises serious concerns about smart contract security. As such, there is an inevitable need to better maintain smart contract code and ensure its high reliability prior to deployment especially smart contracts that are used to create and hold millions of US dollars' worth of digital currencies. A popular standard for such smart contracts on the Ethereum blockchain network is the ERC-20 token standard. The security of these smart contracts is the focus of these chapter by using the source code quality measurements of the chapter as the input in supervised machine learning models to predict the vulnerability contained within each smart contract source code.

Based on this premise, this chapter has the following objectives:

1. Collect a sample of smart contract source code which have already been deployed to the public Ethereum blockchain network via the etherscan blockchain explorer API.
2. Extract the source code attributes/metrics for each smart contract
3. Append the most prevalent identified vulnerability of bug in each smart contract to the software metrics dataset
4. Use the source code metrics and the dependent variable (the vulnerability labels) as the input in supervised machine learning algorithms to create models that can predict a smart contracts vulnerability based on its source code attributes.
5. Compare the accuracy obtained when the machine learning algorithms are used independently and when the algorithms are combined to form an ensemble algorithms/classifier.

BACKGROUND

Blockchain Technology is the technology at the core of the decentralised Bitcoin payment system (with Bitcoin as its native cryptocurrency) as well as the Ethereum blockchain platform (with Ether as its native cryptocurrency). When compared to Bitcoin, Ethereum permits the development and deployment of decentralised and distributed applications called smart contracts (with Solidity being the main programming language for smart contract development) which are self-executed pieces of code that run on the EVM (ethereum virtual machine). Once deployed via a smart contract creation transaction[1], these smart contracts cannot be altered or modified due to the immutable nature of the blockchain technology which does not permit modification of transactions (Li et al., 2017) to prevent people from performing double spending as an example (i.e., double spending 10 bitcoins by transferring to Party A from Party C and sending the same 10 bitcoins in another transaction to Party B from C again while C's initial balance was 10 bitcoins). As such, software with blockchain smart contracts at their core require an effective software development process with security as a top priority.

Various use cases for smart contracts or decentralised applications (as they are called due to the nature of the decentralised blockchain network) have been seen over the years. Including escrow smart contracts, decentralised microinsurance, decentralised finance (with lending and repayments), etc. Most importantly, a more popular use case is the creation of alt coins or alternate coins which are digital currencies built on top of the ethereum blockchain network apart from the native Ether. These digital currencies are alternatives to the native Ether and are created via smart contracts. Some of these have also been used in crowdfunding blockchain-based startups in what is popularly referred to as an Initial Coin Offering (ICO). Just like Ether, these currencies can hold value, be transferred from one part to another and can be received. There are various smart contract standards created by the Ethereum community for creating these alt coins (Liu et al., 2021). A more popular one is the ERC-20 token standard[2] which sets out a specific list of functionalities any ERC-20 alt coin must implement, i.e., three optional (token name, symbol, decimals up to 18) and six compulsory (*totalSupply*, *balanceOf*, *transfer*, *transferFrom*, *approve*, *allowance*) functionalities.

However, depending on the use case for an alt coin, developers might alter the implementations of these required functionalities slightly which in some cases has led to serious attacks and loss of millions of USD worth of alt coins. This has led to the creation of various secure smart contract development libraries providing developers with secure and audited source code templates to build upon. One example is the OpenZeppelin framework[3] with over 200 open source software contributors/ developers on GitHub.

A code snippet of the ERC-20 token standard smart contract from the OpenZeppelin framework is shown below with some of the required functionalities providing a standard way of implementing and interacting with created alt coins or digital currencies on the Ethereum blockchain network:

```
pragma solidity >=0.6.0  <0.8.0;
contract ERC20 is Context, IERC20 {
```

```
             using SafeMath for uint256;
             mapping (address => uint256) private _balances;
             mapping (address => mapping (address => uint256))
private
_allowances;
             uint256 private _totalSupply;
             string private _name;
             string private _symbol;
             uint8 private _decimals;
             constructor (string memory name_, string memory
symbol_)
public {
                       _name = name_;
                       _symbol = symbol_;
                       _decimals = 18;
                      }
              function name() public view returns (string
memory) {
                       return _name;
              }
              function balanceOf(address account) public view
override
returns (uint256) {
                       return _balances[account];
              }
              function transfer(address recipient, uint256
amount)
public virtual  override  returns (bool) {
                       _transfer(_msgSender(), recipient,
amount);
                       return true;
              }
              ---
     }
```

Many bugs and vulnerabilities in such ERC-20 smart contracts (Xu et al., 2021) have led to serious financial losses (e.g., $3 million US dollars[4] equivalent in digital currency lost to a hacker in an incident reported in December 2020), which raises serious concerns about smart contract security. As such, there is an inevitable need to better develop secure smart contract source code and ensure a high reliability.

While source code-based bug prediction has gained traction in the traditional software engineering space, we are yet to see such studies within the blockchain or immutable software space.

Based on this premise, the contributions of this study are as follows: the adoption of OO metrics in the blockchain-oriented software engineering domain; a novel empirical investigation of the link between OO software metrics and ERC-20 smart contracts vulnerabilities, to address the research question - *to what degree can smart contract code metrics predict the exact vulnerability within the code using classification algorithms individually when compared to using an ensemble classifier?* ; a demonstration of using ensemble classifier to obtain better prediction accuracy compared to individual classification algorithms, and ; (publicly available) curated dataset and associated tools[5]

The novelty of the study is in the use of smart contract code quality metrics as input in supervised machine learning models (separately) and an ensemble model (composed of multiple models for better accuracy) to predict the exact vulnerability that a smart contract contains. Another novelty is the focus on ERC-20 smart contract standard used by developers in the Ethereum community to implement alternative digital currencies on top of the Ethereum blockchain. Other studies have analysed smart contracts taking those contracts implementing varying use cases such as decentralised escrows, file integrity checkers, microinsurance, supply chain, etc. using deep learning algorithms in some cases (e.g., Zhuang et al., n.d.) with relatively similar accuracy obtained from their models compared to our ensemble classifier.

The rest of the chapter is structured as follows: the following section outlines the scope of the chapter (its main focus) and methodology. The solutions section goes into more details on the methodology, describes the smart contract source code metrics extracted, the case study (data sample), and the supervised machine learning algorithms used. The results section outlines and discusses the derived results from the machine learning models in terms of Accuracy while the future directions section outlines some ideas for further work. Finally, the conclusion section concludes the study and chapter.

MAIN FOCUS OF THE CHAPTER

The chapter aims to answer the following research question in the context of the ERC-20 token smart contract standard for the Ethereum blockchain network: *to what degree can smart contract code metrics predict the exact vulnerability within the code using classification algorithms individually when compared to using an ensemble classifier*?

The methodology will follow the following steps which are described in more detail in the next section of the chapter:

Step 1: Collect a sample of vulnerable ERC-20 standard Ethereum blockchain smart contract addresses
Step 2: Using the addresses, download the source code of each smart contract via the Etherscan Ethereum blockchain explorer API
Step 3: Parse the source code of each smart contract and extract its source code attributes/metrics
Step 4: Merge the source code metrics and prevalent vulnerability of each smart contract into a single .csv file/dataset
Step 5: Pass this dataset as the input in varying supervised machine learning algorithms to build models capable of predicting the labelled vulnerability contained within the smart contract source code
Step 6: Combine the machine learning algorithms in Step 5. in an ensemble classifier and compare the accuracy of the ensemble classifier to the accuracy derived when the algorithms are used separately in Step 5
Step 7: Publish the dataset and script used in an online repository as a replication package for replication studies or further work

SOLUTIONS AND RECOMMENDATIONS

In this section, the following are described: the smart contract source code metrics extracted from the Solidity files for the study as the independent variables, the vulnerability contained within the smart contract (the dependent variable for which we are trying to predict) and the supervised machine learning (classification) algorithms used (i.e., each individual classifier and the ensemble classifier) and implemented in the Python programming language. Thereafter the results are outlined and discussed.

Study Sample of Vulnerable Smart Contracts

The study sample of vulnerable smart contracts is collected from a publicly available repository of vulnerable ERC-20 token smart contracts[6]. It contains the list of smart contract addresses on the live public Ethereum blockchain network and their associated vulnerabilities to help ERC20 token contract developers to develop correct and secure contracts. The ERC-20 token

as described earlier is the most popular standard for creating custom alternative digital currencies on top of the Ethereum blockchain network for use apart from its native Ether currency used to also pay for transaction costs.

A total of 4,419 smart contract addresses containing buggy source code was collected. The bugs have been categorised into three main categories (A, B and C) described as: (A) Bugs in implementation - code logic, e.g., overflow; (B) Incompatibilities caused by Different Compiler Versions and External Calls, e.g., no return in ERC20 interfaces; and (C) Excessive authorities, e.g. anyone can change owner. In detail each contract within the source code assigned an address on the blockchain network collected for the study contains one or more of the vulnerabilities outlined in Tables 1 and 2 (below) which is the dependent variable to predict in this study using the source code metrics extracted.

Table 1. Full list of smart contract vulnerabilities (Category A)

Class/Label	Vulnerability
A1	batchTransfer overflow
A2	totalsupply overflow
A3	verify invalid by overflow
A4	owner control sell price for overflow
A5	owner overweight token by overflow
A6	owner decrease balance by mint by overflow
A7	excess allocation by overflow
A8	excess mint token by overflow
A9	excess buy token by overflow
A10	verify reverse in transferFrom
A11	PauseTransfer anyone
A12	transferProxy keccak256
A13	approveProxy keccak256
A14	constructor case insensitive
A15	custom fallback bypass ds auth
A16	custom call abuse
A17	setowner anyone
A18	allowAnyone
A19	approve with balance verify
A20	re approve
A21	check effect inconsistency
A22	constructor mistyping
A23	fake burn
A24	getToken anyone
A25	constructor naming error

Table 2. Full list of smart contract vulnerabilities (Category B and C)

Class/Label	Vulnerability
B1	transfer no return
B2	approve no return
B3	transferFrom no return
B4	no decimals
B5	no name
B6	no symbol
B7	no approval
C1	centralAccount transfer anyone

Extracting the Software (Source Code) Metrics

Chidamber and Kemerer (Chidamber & Kemerer, 1994) proposed a set of object-oriented (OO) software metrics[7]. The metrics include coupling between objects (CBO) (Aloysius & Arockiam, 2012), response for a class (RFC), weighted methods per class (WMC), depth of inheritance tree (DIT), number of children (NOC), and lack of cohesion in methods (LCOM). These metrics provide a theoretical framework for software quality.

These metrics become important and relevant when developers and maintainers are required to estimate software quality, evaluate their productivity, mitigate software faults/bugs and minimise maintenance efforts with an estimate of the or fault-prone change-prone software source code or components (Briand et al., 1999; Kitchenham, 2010).

For example, the C&K metrics have been used in prior studies for various software development or maintenance activities, including but not limited to: prediction of software maintainability (Li & Henry, 1993); investigation of class dependencies in object-oriented software (Oliva & Gerosa, 2011); evaluation of the impact of inheriting features from other artefacts or code (Chhikara et al., 2011); evaluation of software comprehension based on its complexity (Counsell et al., 2002); and as features in prediction models that predict failures and defects (D'Ambros et al., 2010), (El Emam et al., 2001), (Radjenović et al., 2013), (Capretz & Xu, 2008). For example, CBO has demonstrated a significant correlation to software quality (including the defect or error-proneness of a class) (Aloysius & Arockiam, 2012), (Basili et al., 1996), (Wilkie & Kitchenham, 2000). In addition to the C&K metrics, Hegedűs investigated the nature of the typical structure of smart contracts in terms of their OO attributes/metrics with additional metrics (Hegedűs, 2019) including SLOC (Source lines of code), LLOC (Logical lines of code), CLOC (Comment lines of code), NF (Number of functions), McCC (McCabe's cyclomatic complexity (McCabe, 1976)), NL (Nesting level), NLE (Nesting level without else-if), NUMPAR (Number of parameters), NOS (Number of statements), NOA (Number of ancestors), NA (Number of attributes or states), and NOI (Number of outgoing invocations, i.e., fan-out).

Establishing the importance of these metrics in this context, i.e., identifying a significant link between these software metrics and the types of faults existing within the smart contract Solidity source code files will be beneficial for the blockchain community especially as it will help to identify exactly what files and what type of vulnerabilities to focus on before deploying the smart contracts to the blockchain network where they cannot be modified once deployed and a constant address or location has been created for them on the blockchain.

In addition to the C&K metrics (Chidamber & Kemerer, 1994), this preliminary study adopts the metrics suite used in the study titled Towards analyzing the complexity landscape of solidity based ethereum smart contracts by Hegedűs (Hegedűs, 2019) (see the full list of metrics below). We have also adopted the SolMet tool implemented in Java and provided in (Hegedűs, 2019) for the parsing of the smart contracts and extraction of the OO metrics. To summarise, the studied smart contract software metrics include:

- SLOC: source lines of code.
- LLOC: logical lines of code.
- CLOC: comment only lines of code.
- NF: number of functions.
- McCC: McCabe's cyclomatic complexity of the functions.
- NL: sum of the deepest nesting level of the control structures within functions.
- NLE: nesting level without else-if.
- NUMPAR: number of parameters per function.
- NOS: number of statements.
- NOA: number of ancestors.
- WMC: weighted methods per class.
- DIT: depth of inheritance tree.
- CBO: coupling between objects.
- NA: number of attributes or state variables).
- NOI: number of outgoing invocations or functions called from a function in a smart contract.
- Average NL.
- Average NLE.
- Average NUMPAR; and lastly,
- Average NOS.

Once the smart contract addresses were collected, we proceeded to download the smart contract source code from the blockchain network via an API provided by the Etherscan Ethereum blockchain network explorer to a local PC. With the verified smart contract files containing one or more smart contract source code (i.e., the ERC-20 contracts and their dependencies) we extracted the software metrics using the SolMet tool implemented in Java and provided in (Hegedűs, 2019). This gave us the metrics described above for each smart contract within the downloaded Solidity source code files. A total of 10,476 individual smart contracts were identified and parsed by the tool. For each smart contract, we merged the source code metrics (independent attributes/variables) and the dominant vulnerability (dependent attribute to predict) from the list of vulnerabilities listed in Tables 1 and 2 into a .csv file as the input for the selected supervised machine learning algorithms described below.

Supervised Machine Learning Algorithms (Classifiers)

Scikit-learn (Pedregosa et al., 2011) is a Python package consisting of a variety of the latest machine learning algorithms for supervised and unsupervised problems. It enables non-programming experts perform machine learning tasks with a focus on ease of use, high performance, documentation and API consistency. It has been used widely in commercial and academic settings as well (Abraham et al., 2014).

As this study focuses on a supervised learning problem, we have adopted three widely used classification algorithms within the Scikit-learn package individually (based on their strengths as described in prior work (Pratama & Sarno, 2015)) namely: KNN, Multinomial Naive Bayes and Random Forest. In addition, these three algorithms have also been combined in an ensemble classifier (namely Voting) to determine the accuracy when using them separately and collaboratively.

K-Nearest Neighbors (KNN) is a classification algorithm that makes use of a distance function between the train data to test data as well as the number of nearest neighbours to identify the classification outcomes. The distance function used in this experiment is the Euclidean distance between the data points. The nearest neighbor in this case is the smart contract with similar software metrics (which means that there is a likelihood that it will contain the same vulnerability). We have tuned the

n_neighbors parameter for KNN in Scikit-learn to being an iterative process to find a suitable number of neighbors to learn from for better accuracy.

Naive Bayes is a classification algorithm based on the application of the Bayes theorem. Multinomial Naive Bayes (MNB) is a variation of the Naive Bayes designed to solve the classification of text documents. MNB uses multinomial distribution with the number of occurrences of a word or the weight of the word as a classification feature. On the other hand, the Gaussian naive Bayes classification is a case of naive Bayes method with an assumption of having a Gaussian distribution on attribute values given the class label (smart contract vulnerability in this case) (Jahromi & Taheri, 2017). As we cannot assume a Gaussian distribution for the independent variables in the dataset (source code metrics), the Multinomial NB has been adopted. The have also both been tried for selection and Multinomial NB performed better than Gaussian NB on the dataset.

Random Forest classifier consists of a combination of tree classifiers where each classifier is generated using a random vector sampled independently from the input vector, and each tree casts a unit vote for the most popular class to classify an input vector (Pal, 2005). This classifier has been shown to have better accuracy over single tree classifiers such as the Decision tree (or J48) classifier.

An ensemble of classifiers is a set of classifiers whose individual decisions are combined in some way (typically by weighted or unweighted voting) to classify new examples. In the Scikit-learn package, the Voting ensemble classifier has been adopted for this study (Dietterich, 2000) and a hard voting has been used which takes the class or dependent variable with the highest votes among the classifiers as the predicted class or dependent variable.

More Issues, Controversies, Problems

In this section the results derived from the classification algorithms are presented and their impact on smart contract development and security is discussed.

Using Scikit-learn function for randomly splitting the data into a 50-50 training and testing subset, each of the classifiers was trained using a subset of the dataset containing the source code metrics (independent variables) for each smart contract and the prevalent vulnerability within the smart contract (dependent variable/class to predict). The generated prediction models were then evaluated in terms of their accuracy score (e.g., as shown in the source code below for the Multinomial Naive Bayes Classifier) on the test subset of the dataset to determine their performance in using the source code metrics as predictors of the category of vulnerability that a smart contract contains. Accuracy has been used as an evaluation metric, because we are dealing with vulnerabilities which can have serious effects if exploited. Therefore, in this case the True Positives and True negatives are more important while F-score is used when the False Negatives and False Positives are crucial.

```
#Multinomial Naive Bayes classifier
from sklearn.naive_bayes import MultinomialNB
mnb = MultinomialNB().fit(X_train, y_train)
mnb_predictions = mnb.predict(X_test)
#evaluate accuracy on X_test
accuracy = mnb.score(X_test, y_test)
```

```
print(accuracy)
#creating a confusion  matrix
cm = confusion_matrix(y_test, mnb_predictions)
```

The formula for accuracy is presented in equation below:

$$Accuracy = \frac{True\,Positive + True\,Negative}{\left(True\,Positive + False\,Positive + True\,Negative + False\,Negative\right)}$$

Table 3. Supervised machine learning results

ID	Classification Algorithm	Accuracy
1	KNN	0.69
2	Multinomial Naïve Bayes (NB)	0.13
3	Random Forest	0.78
4	Voting (Ensemble Classifier composed of KNN, Multinomial NB, and Random Forest classifiers)	0.79

The accuracy scores for each individual classifier and the ensemble (Voting) classifier are shown in Table 3 (above). As shown, the ensemble classifier outperforms the other three algorithms used in predicting the vulnerability contained within the smart contract source code. Using a combination of the three individual algorithms in an ensemble classifier or supervised machine learning model, we can predict exactly the vulnerability category contained within a smart contracts source code prior to deploying the smart contract.

These results are significant in practice for the smart contract development community as it implies that we can have safer and secure smart contracts and specifically know exactly what vulnerability to look out for when debugging for vulnerabilities or bugs. This will also lead to targeted efforts which will save smart contract developers time and potentially millions of funds lost in ERC-20 smart contract hacks as see in the past. Other researchers are encouraged to use the datasets provided in their prediction models to explore achieving a better/improved accuracy.

Therefore, this section can be concluded with an answer the research question: *to what degree can smart contract code metrics predict the exact vulnerability* *within the code using classification algorithms individually when compared to using an ensemble classifier*? which is that using source code metrics to predict the vulnerability contained within smart contracts is a feasible effort and can be achieved to a significant degree with significant accuracy.

FUTURE RESEARCH DIRECTIONS

Discuss future and emerging trends. Provide insight about the future of the book's theme from the perspective of the chapter focus. Viability of a paradigm, model, implementation issues of proposed programs, etc., may be included in this section. If appropriate, suggest future research opportunities within the domain of the topic.

As further work, performing fine-grained predictions, i.e., going from the smart contract level down to predicting exactly which method or feature has a specific vulnerability is a feasible research effort. Another plan for further work will be to conduct a multi label classification i.e., to predict not just one but multiple vulnerabilities out a set of vulnerabilities present in the ERC-20 smart contracts. Lastly, integrating these machine learning models into IDEs (integrated development environments) for real-time vulnerability prediction is an ideal work for the future as it will save developers time by predicting these vulnerabilities at development time rather than after compilation and deployment.

CONCLUSION

Section title should be "Conclusion," not "Conclusions." Provide discussion of the overall coverage of the chapter and concluding remarks.

In summary, this study has explored the use of smart contract source code/ structural attributes in the prediction of the type of vulnerability or bug contained within the code. Three supervised machine learning algorithms were used, namely: KNN, Random Forest and Multinomial Naive Bayes. In addition, these algorithms were combined in an ensemble classifier namely Voting to determine if they perform better individually or together based on a majority votes mechanism. The results derived were impressive and significant showing that the ensemble classifier outperformed the three algorithms when applied independently of each other. The ensemble classifier showed an accuracy score of 79% followed by Random Forest with an accuracy score of 78%.

These methodology and results are significant for practitioners, particularly for the smart contract development community implementing digital currencies or tokens for the Ethereum blockchain network based on Ethereum's ERC-20 token standard as it shows the feasibility of identifying specifically the type of vulnerability contained within a smart contract. Thus, enabling a targeting smart contract security analysis and fixing potentially saving developers and owners of blockchain oriented projects millions of US dollars' worth of digital currencies in the event of a hack as seen in the past.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Abraham, A., Pedregosa, F., Eickenberg, M., Gervais, P., Mueller, A., Kossaifi, J., Gramfort, A., Thirion, B., & Varoquaux, G. (2014). Machine learning for neuroimaging with scikit-learn. *Frontiers in Neuroinformatics*, *8*, 14. doi:10.3389/fninf.2014.00014 PMID:24600388

Aloysius, A., & Arockiam, L. (2012). Coupling complexity metric: A cognitive approach. *International Journal of Information Technology and Computer Science*, *4*(9), 29–35. doi:10.5815/ijitcs.2012.09.04

Basili, V. R., Briand, L. C., & Melo, W. L. (1996). A validation of object-oriented design metrics as quality indicators. *IEEE Transactions on Software Engineering*, *22*(10), 751–761. doi:10.1109/32.544352

Briand, L. C., Daly, J. W., & Wüst, J. K. (1999). A unified framework for coupling measurement in object-oriented systems. *IEEE Transactions on Software Engineering*, *25*(1), 91–121. doi:10.1109/32.748920

Capretz, L. F., & Xu, J. (2008). An empirical validation of object-oriented design metrics for fault prediction. *Journal of Computational Science*, *4*(7), 571–577. doi:10.3844/jcssp.2008.571.577

Chhikara, A., Chhillar, R., & Khatri, S. (2011). Evaluating the impact of different types of inheritance on the object oriented software metrics. *International Journal of Enterprise Computing and Business Systems*, *1*(2), 1–7.

Chidamber, S. R., & Kemerer, C. F. (1994). A metrics suite for object oriented design. *IEEE Transactions on Software Engineering*, *20*(6), 476–493. doi:10.1109/32.295895

Counsell, S., Mendes, E., & Swift, S. (2002). Comprehension of object-oriented software cohesion: The empirical quagmire. *Proceedings of the 10th International Workshop on Program Comprehension (IWPC)*, 33–42. 10.1109/WPC.2002.1021308

D'Ambros, M., Lanza, M., & Robbes, R. (2010). An extensive comparison of bug prediction approaches. *7th IEEE Working Conference on Mining Software Repositories (MSR)*, 31–41. 10.1109/MSR.2010.5463279

Dietterich, T. G. (2000). Ensemble methods in machine learning. *International workshop on multiple classifier systems*, 1–15. 10.1007/3-540-45014-9_1

Ebert, C., Cain, J., Antoniol, G., Counsell, S., & Laplante, P. (2016). Cyclomatic complexity. *IEEE Software*, *33*(6), 27–29. doi:10.1109/MS.2016.147

El Emam, K., Melo, W., & Machado, J. C. (2001). The prediction of faulty classes using object-oriented design metrics. *Journal of Systems and Software*, *56*(1), 63–75.

Hegedűs, P. (2019). Towards analyzing the complexity landscape of solidity based ethereum smart contracts. *Technologies*, *7*(1), 6.

Jahromi, A. H., & Taheri, M. (2017). A non-parametric mixture of gaussian naive bayes classifiers based on local independent features. *2017 Artificial Intelligence and Signal Processing Conference (AISP)*, 209–212. 10.1109/AISP.2017.8324083

Kitchenham, B. (2010). What's up with software metrics? –A preliminary mapping study. *Journal of Systems and Software*, *83*(1), 37–51. doi:10.1016/j.jss.2009.06.041

Li, W., & Henry, S. (1993). Object-oriented metrics that predict maintainability. *Journal of Systems and Software*, *23*(2), 111–122. doi:10.1016/0164-1212(93)90077-B

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*.

Liu, Z., Qian, P., Wang, X., Zhuang, Y., Qiu, L., & Wang, X. (2021). Combining graph neural networks with expert knowledge for smart contract vulnerability detection. *IEEE Transactions on Knowledge and Data Engineering*, 1. doi:10.1109/TKDE.2021.3095196

McCabe, T. J. (1976). A complexity measure. *IEEE Transactions on Software Engineering*, *SE-2*(4), 308–320. doi:10.1109/TSE.1976.233837

Oliva, G. A., & Gerosa, M. A. (2011). On the interplay between structural and logical dependencies in open-source software. *25th Brazilian Symposium on Software Engineering (SBES)*, 144–153. 10.1109/SBES.2011.39

Pal, M. (2005). Random forest classifier for remote sensing classification. *International Journal of Remote Sensing*, *26*(1), 217–222. doi:10.1080/01431160412331269698

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., & Dubourg, V. (2011). Scikit-learn: Machine learning in python. *Journal of Machine Learning Research, 12*, 2825–2830.

Pratama, B. Y., & Sarno, R. (2015). Personality classification based on twitter text using naive bayes, knn and svm. *2015 International Conference on Data and Software Engineering (ICoDSE)*, 170–174. 10.1109/ICODSE.2015.7436992

Radjenović, D., Heričko, M., Torkar, R., & Živkovič, A. (2013). Software fault prediction metrics: A systematic literature review. *Information and Software Technology*, *55*(8), 1397–1418. doi:10.1016/j.infsof.2013.02.009

Wilkie, F. G., & Kitchenham, B. A. (2000). Coupling measures and change ripples in C++ application software. *Journal of Systems and Software*, *52*(2-3), 157–164. doi:10.1016/S0164-1212(99)00142-9

Xu, Y., Hu, G., You, L., & Cao, C. (2021). A Novel Machine Learning-Based Analysis Model for Smart Contract Vulnerability. *Security and Communication Networks*, *2021*, 2021. doi:10.1155/2021/5798033

Zhuang, Y., Liu, Z., Qian, P., Liu, Q., Wang, X. & He, Q. (n.d.). *Smart contract vulnerability detection using graph neural networks*. Academic Press.

KEY TERMS AND DEFINITIONS

Alt Coin: A cryptocurrency other than bitcoin or ether built on top of the Ethereum blockchain network via smart contract source code.

Cryptocurrency: A digital currency whose security is guaranteed through the use of cryptography.

Decentralised: No central authority.

Decentralised Autonomous Organisation (DAO): A new type of self-governing organisation that leverages smart contracts on the Ethereum blockchain. In return for their early support, participants receive DAO tokens that allow them to vote on important decisions.

ERC-20 Token Standard: ERC-20 has emerged as the technical standard; it is used for all smart contracts on the Ethereum blockchain for token implementation and provides a list of rules that all Ethereum-based tokens must follow.

Ether: The cryptocurrency used on the Ethereum blockchain.

Ethereum: A blockchain that runs smart contracts using its own cryptocurrency, the Ether.

Public Blockchain Network: A blockchain that grants read access and ability to create transactions to all users.

Smart Contract: A contractual agreement built on computer protocols, whose terms can be executed automatically.

ENDNOTES

[1] An example smart contract creation transaction can be viewed on the etherscan Ethereum blockchain network explorer at: https://etherscan.io/tx/0xc1bb88fbc915034f4e719fdc58c8896ef5f38e50244c990b03946a3fc6ec21c0

[2] A list of the top ERC-20 tokens on the ethereum blockchain network can be found at: https://etherscan.io/tokens

[3] https://github.com/OpenZeppelin/openzeppelin-contracts

[4] https://coingeek.com/nexus-mutual-attacker-cashes-out-3-million/

[5] The dataset and tool or script used to perform the supervised ensemble and non-ensemble classifications for this study are publicly available at: https://figshare.com/articles/dataset/Supervised_machine_learning_for_smart_contract_vulnerability_prediction/13417316

[6] The sample can be found at: https://github.com/sec-bit/awesome-buggy-erc20-tokens

[7] Commonly called Chidamber and Kemerer Java Metrics (CKJM) or C&K.

Chapter 7

An Application-Oriented Survey on the Adaptability of Artificial Intelligence for Natural Language Processing: A Survey

Surya Teja Marella
https://orcid.org/0000-0002-3790-7955
Western Michigan University, USA

Guan Yue Hong
Western Michigan University, USA

ABSTRACT

The application domains for artificial intelligence and machine learning are expanding exponentially in recent times. The domains such as automation in software and business processes, healthcare, agriculture, robotics, and mostly natural language processing have seen the most adaptations. The domain of natural language processing seeks the maximum adaptation due to various sub domain applications such as textual classification, detection of emotions, design and delivery of virtual assistant tools, extraction of knowledge, content summarization, content recommendations, user profiling for content consumption habits, grammar and dialect verification, and text summation. These subdomains cater to a wide range of purposes such as user profiling or emotion extraction for surveying or feedback analysis for data-driven applications.

DOI: 10.4018/978-1-6684-3855-8.ch007

INTRODUCTION

Natural Language Processing (NLP) is the field of study that enables machines to analyze, understand, generate, and manipulate human languages. When you take Artificial Intelligence and focus it on human linguistics, you get NLP. NLP infuses the power of linguistics with computational capabilities, studies the rules and structure of language, enabling machines to understand, analyze, extract meaning from text and speech. Take Gmail, for example. Thanks to an NLP process called keyword extraction, all emails are automatically classified as Primary, Promotions, Social, or Spam. By extracting words from the subject of the emails, NLP categorizes them based on their associations to predefined 'tags', and thereby automatically "learns" which category to assign an email to.

NLP works on the basic idea that humans operate by internal 'maps' of their surroundings and learn through sensory data. NLP tries to detect and implement the conscious use of language to interpret what we are 'thinking' rather than simply 'saying'.

Natural language processing enables machines to extract keywords and phrases, understand the intentions of sentences, translate them to another language, or generate a human-like response. Using vectorization, NLP transforms text or voice into a machine-understandable format, feeds it to machine learning algorithms as sets of training data with tags or labels to enable machines to make associations between languages and human behaviours (Young et al. 2018).

When we consider a sentence, we are talking about syntax, semantics, tense and conversation. For a machine to understand human language, it must understand all these aspects of a simple sentence and also in what context they are being referred to, which might seem overwhelming due to the number of rules it needs to track. This explains why the early attempts at NLP underperformed. However, significant contributions over the past few decades have yielded state-of-the-art results for even common NLP tasks.

NLP has been a game-changer in each and every aspect of our lives. Be it the predictive texts like autocorrect, autocomplete, smart assistants like Alexa or Siri, automatic summarization, Named Entity Recognition, sentiment analysis, speech recognition, topic segmentation, or email filtering, NLP has truly changed how we interact with machines.

Table 1. Abbreviations used in the paper.

Variable	Meaning
NLP	Natural Language Processing
NLU	Natural Language Understanding
NLG	Natural Language Generation
cTAKES	clinical Text Analysis and Knowledge Extraction System
POS	Part-of-speech tagger
NER	Named Entity Recognition
CRF	Conditional Random Fields

Components of NLP

NLP is divided into two basic components:

- Natural Language Understanding
- Natural Language Generation

Natural Language Understanding (NLU)

When dealing with interpreting language there are a lot of ambiguities. lexical ambiguity occurs when the semantic (meaning) of a word is different depending on the sentence it is used in. 'the priest *married* my sister' is a perfect example of lexical ambiguity. Syntactical Ambiguity is when a sequence of words carries different meanings. 'The chicken *is ready* to eat' – is the chicken ready to eat his food or is it ready for someone else to eat? Referential Ambiguity occurs when a text mentions something/someone using a particular word and then references them again, in another sentence, using another word.

NLU analyses sentences to determine their meaning and reduce them into structured ontology, i.e., a format consisting of semantics and pragmatics. Intent and entity recognition are the fundamental concepts of NLU.

Intent recognition identifies the sentiment of the speaker in the given input and determines their objectives. Whereas, entity recognition deals with isolating entities in input and classifying them either as people, locations, names (named entities), or as numbers, percentages (numeric entities). The main purpose of NLU is to understand the meaning of these inputs despite human errors.

Natural Language Generation (NLG)

The Natural Language Generation (NLG) is the process of machines automatically generating natural text, similar to the way we naturally communicate. Usually, machine-generated content, overall, lacks the flow, emotion, and personality that make human-created content intriguing and engaging. NLG overcomes this limitation to produce human-like text, emulating a human writer.
There are three phases usually involved in NLG:

1. Text planning – obtaining appropriate content from the existing knowledge base.
2. Sentence planning – entails selecting necessary words, generating meaningful phrases, and determining the tone of the sentence.
3. Text Realisation – mapping of a sentence plan into a sentence structure.

Observations

1. Bayesian network models for hierarchical text classification.

Text classifiers help organize data and provide quick access to relevant information. They are used universally, and each has its own constraints to classify different kinds of data. Although these sets of rules can be automated, however, as pointed out by researchers, De Campos and Romero (2009), in their paper titled "*Bayesian network models for hierarchical text classification from a thesaurus*", it is unrealistic to attempt designing a completely automatic classification process due to the critical nature of classification tasks and human intervention will always be required in any real-world applications.

Therefore, De Campos and Romero (2009) proposed a method that automatically generates a set of descriptors extracted from a thesaurus, using Bayesian network and probabilistic inferences to choose these descriptors, delivering a high accuracy of classifying topics relevant to the descriptor. The highlight of their method is that it wouldn't require any training. They began with using only lexical and hierarchical information from the thesaurus which ensured that a large training data set would not be required for the model. However, this came at the cost of omitting other relations from the thesaurus and therefore led to a lower accuracy rate. Nevertheless, the model can naturally utilize training data to improve performance. The pre-classified documents along with the hierarchical and equivalence relationships of the descriptors would in turn deliver a better classifier system.

They used Bayesian networks to model the equivalence and hierarchical information relationships. Once the document to be classified is instantiated in the model, a probabilistic inference algorithm computes the posterior possibilities of the generated descriptors. The Bayesian Network model itself is extended to use training data. To explicitly distinguish between concepts and descriptors and non-descriptors, each concept which is labeled as the descriptor representing it, is represented as a node in the network. To clearly separate the different information sources influencing the concept, for each concept node, two virtual nodes are created which will receive information provided by the equivalence and hierarchical relationships influencing the concepts contained in the concept nodes. For the links, there is an arc from each term node to the descriptors and/or non-descriptor nodes containing it. There are arcs that are present between each non-descriptor node and the virtual nodes as well as their own descriptor nodes associated with the concept. Finally, there are arcs from the virtual equivalence relationship nodes and hierarchical relationship nodes to their associated concept node, representing that the relevance of a given concept will directly depend on the information provided by the equivalence node and the hierarchical node relationships. Next, the conditional probabilities for every type of node are specified.

Pre-classified documents are included into the Bayesian network model, thus obtaining a supervised classifier. Following up the previously used idea of clearly separating the different sources of information relative to each concept, a new parent node, called virtual training node is added to each concept node (in addition to those virtual nodes representing hierarchical and equivalence relationships), representing the information obtained for this concept from the training documents. In other words, this new parent node will contain the posterior probability distribution for the relevance of the concept, predicted by a (probabilistic) supervised classifier. An OR gate will be used to merge the information gathered from the hierarchy and equivalence nodes.

The created model was tested against different experimental evaluations. The evaluation took into account that the aim is not complete but only partial automation of the classification process, showing to the user an ordered list of the most probable descriptors. Performance measures like breakeven point, F1 measure and the average, 11-point precision were used. They carried out the experiments in two scenarios: without using training documents and with using training documents. The model without training evidently outperformed the two simple benchmark methods they considered to compare their model with. By integrating the initial model within a more general scheme where training data, in the form of pre-classified documents, may also be used, the model also outperformed standard text classification algorithms, such as Rocchio and Naive Bayes, obtaining results comparable to those of support vector machines.

2. Mayo clinical Text Analysis and Knowledge Extraction System (cTAKES).

Finding meaning from text is Semantic analysis. It involves analyzing entire documents, paragraphs, and sentences to interpret their meaning. The semantic analysis process involves more than just finding the dictionary meaning of words in a sentence. It checks for the meaningfulness of text by understanding the grammatical structure, relationships between words, and other processes. The cTAKES - *Mayo clinical Text Analysis and Knowledge Extraction System (cTAKES)*, proposed by Savova et al. (2009), provides the base for higher-level semantic processing of clinical free-text. They designed a scalable NLP system to extract semantically viable data from digital medical record clinical texts for supporting heterogeneous clinical research. Clinical narratives have unique features that distinguish them from normal biomedical literature and hence require special methods to perform semantic analysis.

For information extraction from the clinical narrative, cTAKES implements machine learning and rule-based techniques. It is an incremental model that integrates with the cumulative annotation dataset. cTAKES is built using the OpenNLP toolkit ("Apache OpenNLP", n.d.) and Unstructured Information Management Architecture framework. These frameworks consist of various components:

- Sentence boundary detector
- Tokenizer
- Normalizer
- Part-of-speech (POS) tagger
- Shallow parser
- Named entity recognition (NER)

cTAKES implements a normalizer wrapper to enable mapping of multiple mentions of the same word, not having the same string representation. The wrapper wraps around a SPECIALIST Lexical tool ("Lexical Variant Generation (LVG)", n.d.). Both normalized and non-normalized forms are used by the dictionary look-up method they created. The cTAKES' NER component uses a terminology-agnostic dictionary lookup algorithm and each word is mapped to concepts described in the terminology. The algorithm takes the output from the shallow parser and the noun phrases become look-up windows. Non-lexical variations are accounted for by checking all permutations of heads and modifiers within the noun phrases. Ambiguity in multiple terms in the same text span is not resolved by the NER. The status and negation annotator uses the NegEx algorithm (Skeppstedt, 2011) for finding related words and entities. Certain attributes such as the text span in relation to the named entity (whether the named entity is negated or not), the status of the entity, along with the semantic types were selected after consulting clinical researchers and frequent UMLS types and groups were disordered (“Unified Medical Language System (UMLS)”, n.d.). The status is set to ‘possible’ for any future events as they are considered hypothetical.

Although the cTAKES is prompt, the dictionary NER look-up needs to maintain a lexical variant dictionary and it fails to recognize complex levels of synonymy.

3. Identifying sources of opinions with conditional random fields and extraction patterns.

Sentiment analysis is related to finding emotions or tone behind texts, generally in the form of opinions. Sentiment classification aims at classifying opinions’ polarity as either positive, negative or neutral. Choi et al. (2005) went a step further to explore the direct and indirect sources of opinions, sentiments and emotions themselves, and other private states that are expressed in texts. They undertook this task as information extraction. Information Extraction (IE) handles source identification by treating an opinion statement as a kind of speech event, considering the source as the agent. Graphical model and extraction pattern learning methods are also used. They combined Conditional Random Fields (CRF) and a modified AutoSlog to achieve results. CRF models source identification by sequence tagging and AutoSlog was used to extract patterns. While CRFs approached source identification as a sequence tagging problem, AutoSlog treated it as a pattern-matching one. The combination of these two techniques performed better than each individually.

For sequence tagging, a linear-chain is created based on undirected graphs. For each sentence, a non-negative clique expression is defined, separately for each edge and each node. A binary feature indicator function is added as a weight bias. For developing features, Choi et al. (2005) observed that the sources of opinions are usually noun phrases, semantic entities and directly related to opinion expressions. Considering all three factors together, the task becomes complex as sophisticated encoding of sentence structure needs to be incorporated to capture relationships between sources and expressions. Considering all these factors, binarized features were fed to the CRF model for each word/token. Capitalization features, parts-of-speech features, opinion lexical features and dependency trees features are defined and included for the source identification task.

Statistical adaptation of AutoSlog IE learning-algorithm is used to extract opinion sources. AutoSlog’s heuristics were combined with statistically annotated training data to build a fully automated system that does not depend on manual testing. This enhanced statistical process included 3 steps.

- AutoSlog's heuristics were implemented to generate extraction patterns for each noun phrase.
- These learned patterns are legitimized using semantic selectional restrictions.
- Finally, the patterns were trained and statistics were gathered about their extractions.

For testing the model, they used the Multi-Perspective Question Answering corpus (Stoyanov et al., 2005). The corpus consists of documents annotated with opinion-related sources. These documents were split into tuning sets and the rest were used for evaluations as well. Testing was done using three parameters.

- Overlap Match (OL) – this is the most lenient parameter of the three which returns a positive if any extractions match with the words in the document.
- Head Match (HM) – a more conservative measure that matches the heads of the extracted word and the annotated document words.
- Exact Match (EM) – this is the strictest parameter that requires an exact match between the annotated and the extracted word.

Recall – weighted, precision – weighted and F -measure were the evaluation metrics used. Two baseline systems were developed to test the model. The first baseline system labels words according to the respective semantic categories like human, government etc. The calculated precision was low reinstating that opinion recognition is key for source identification. The recall is limited due to the magnitude of the unrecognized semantic categories. The second baseline system marked nouns as sources if either of these conditions were true: The word is a subject of a verb, follows "according to"; is preceded by opinion words and contains a possessive; attaches to an opinion word and follows "by".

These two baselines ensured that the features conditions defined were met. Tabulated data showed that the precision for these baseline models was the highest, although the recalls were low. Learned extraction patterns were applied to the test documents and the results showed that these patterns alone were able to recognize almost half of the opinion sources with a very high precision rate, recall still being low. To overcome the limitation of the CRF model which is unable to form feature boundaries, they added conjunctive features and used the feature induction approach introduced by McCallum (2003). This showed consistently improved performance as conjunctive features were being automatically generated.

Error analysis highlighted some common factors in the mistakes. Error propagation was caused by the non-formation of the dependency tree information. Unusual and complex sentence structures weren't being captured by the simple CRF encoding.

The limited coverage of the opinion lexicon failed to recognize idiomatic and vague expressions.

The developed system had an accuracy of 79.3% while identifying opinion sources with 79.3% and 59.5% recall using a head noun matching measure, and 81.2% precision and 60.6% recall using an overlap measure.

CONCLUSION

Distributed representation has enabled Deep Learning to become the technology driving NLP. Supervised learning is currently the technology that is working best with NLP. However, nothing usually is labelled in the real world where we need to apply NLP techniques. Advanced supervised or semi-supervised approaches are required to implement NLP to enable it to deal with real-world scenarios. We need to start implementing newer techniques for training, like the zero-shot learning algorithm, even though they are in their early stages of development in order to drive deep learning based NLPs to make better use of unlabelled data.

NLP predicts the next tokens using the immediate token history. Augmenting neural language models with attention span mechanisms over differential memory is a recently proposed technique. This model queries the immediate history in memory to predict the next token, however, it is observed that a single vector output is achieved per step. Almost all neural network models are found to be using only the most recent history and fail to utilize long-range dependencies. In fact, much simpler RNN models seem to use output data from the previous three steps and perform at power with sophisticated memory-augmentation NL models. Therefore, there is a need to see more deep learning models with external memories, enriching the internal memory.

Symbolic and sub-symbolic artificial intelligence will play a key role in advancing from NLP to natural language understanding. Machine learning only performs statistical analysis of the data and simply lacks the theoretical insights into natural languages.

REFERENCES

Apache OpenNLP. (n.d.). Retrieved March 26, 2022, from https://opennlp.apache.org/

Choi, Y., Cardie, C., Riloff, E., & Patwardhan, S. (2005). Identifying sources of opinions with conditional random fields and extraction patterns. *Proceedings of human language technology conference and conference on empirical methods in natural language processing*, 355-362. 10.3115/1220575.1220620

De Campos, L. M., & Romero, A. E. (2009). Bayesian network models for hierarchical text classification from a thesaurus. *International Journal of Approximate Reasoning*, *50*(7), 932–944. doi:10.1016/j.ijar.2008.10.006

Lexical Variant Generation (LVG). (n.d.). Retrieved March 26, 2022, from https://www.nlm.nih.gov/research/umls/new_users/online_learning/LEX_004.html

McCallum, A. (2003). Efficiently inducing features of conditional random fields. *UAI'03: Proceedings of the Nineteenth Conference on Uncertainty in Artificial Intelligence*, 403–410.

Savova, G. K., Masanz, J. J., Ogren, P. V., Zheng, J., Sohn, S., Kipper-Schuler, K. C., & Chute, C. G. (2010). Mayo clinical Text Analysis and Knowledge Extraction System (cTAKES): Architecture, component evaluation and applications. *Journal of the American Medical Informatics Association: JAMIA*, *17*(5), 507–513. doi:10.1136/jamia.2009.001560 PMID:20819853

Skeppstedt, M. (2011). Negation detection in Swedish clinical text: An adaption of NegEx to Swedish. *Journal of Biomedical Semantics*, *2*(Suppl 3). doi:10.1186/2041-1480-2-S3-S3 PMID:21992616

Stoyanov, V., Cardie, C., & Wiebe, J. (2005). Multi-perspective question answering using the OpQA corpus. *HLT '05: Proceedings of the conference on Human Language Technology and Empirical Methods in Natural Language Processing*, 923–930. 10.3115/1220575.1220691

Unified Medical Language System (UMLS) at National Library of Medicine. (n.d.). Retrieved March 26, 2022, from https://www.nlm.nih.gov/research/umls/index.html

Young, T., Hazarika, D., Poria, S., & Cambria, E. (2018). Recent trends in deep learning based natural language processing. *IEEE Computational Intelligence Magazine*, *13*(3), 55–75. doi:10.1109/MCI.2018.2840738

Section 2

Electronic Science and Engineering

Chapter 8
RF/Microwave Instruments Evolution:
From Professional Hardware Into Amateur Kit and Software-Defined Radio

Kok Yeow You
https://orcid.org/0000-0001-5214-7571
Universiti Teknologi Malaysia, Malaysia

Yeng Seng Lee
https://orcid.org/0000-0003-3395-7338
Universiti Malaysia Perlis, Malaysia

ABSTRACT

This chapter describes the evolution of RF/microwave instruments within two decades. The described RF/microwave instruments focus more on low-cost amateur RF signal sources, power detectors, spectrum analyzers (SA), vector network analyzers (VNA), and software-defined radios (SDR). Each instrument is introduced, and its uses are compared. This chapter reviews in detail the development history and development factors of amateur RF/microwave instruments in the past 20 years. Through this chapter, fresh RF/microwave amateurs and hobbyists will better understand the development of low-cost instruments in the present and also in the future, as well as provide guidelines for RF/microwave amateurs and hobbyists in the selection and purchase of such instruments. In fact, some amateur instruments are also used in 5G researches and IoT applications when considering their instrument size, research budget, and the need to use a large number of instruments in the application.

DOI: 10.4018/978-1-6684-3855-8.ch008

INTRODUCTION

Recently, RF/microwave technologies have been widely implemented and have become indispensable necessities in our daily work, such as 4G/5G communication network, Internet of Things (IoT), Wi-Fi, Bluetooth, mobile phone, Internet, QR code of personal whereabouts record during the coronavirus (COVID-19) pandemic, and RFID-based security system in work offices. In addition, IoT (operating frequency range from a few hundred MHz to 7.125 GHz) has been broadly applied to different public and industrial fields including machine health monitoring, Industry 4.0, asset monitoring, agriculture monitoring system, asset tracking, environmental monitoring/control, machine-to-machine (M2M), autonomous driving, vehicle to everything (V2X), and delivery truck tracking, passenger car tracking, route development. Therefore, future electrical and electronic engineers will inevitably get involved directly or indirectly in the field of telecommunications.

At the same time, the development of monolithic microwave integrated circuit (MMIC) and microprocessor technology has become increasingly mature and improved in terms of operating frequency, bandwidth, transmit/receive RF power limitation, thermal resistivity, baud rate, power consumption, and several functionalities. The integration of MMIC and programmable microprocessor with the assistance of software can produce software-defined based RF instrument, so-called software-defined radio (SDR), which can be used for the above-mentioned applications. Hence, the use of MMIC components becomes more common, demand increases, and mass production, prices have reached an affordable level. On the other hand, the programmable microprocessors or devices, such as application specific integrated circuit (ASIC), field programmable gate array (FPGA), digital signal processor (DSP), and general purpose processor (GPP), allows the production of higher quality, compact, and cost-effective multi-function SDR.

This has attracted many RF/microwave communication amateurs, enthusiasts, and emerging companies to participate in the development of SDR, such as USB-based RF signal source, portable power sensor, PC-controlled RF transceiver, amateur spectrum analyser (SA), and compact PC-based vector network analyser (VNA) in the past two decades. The USB-based amateur RF test instrument was initially launched on a small scale in 2005, with an operating frequency of up to 100 MHz, such as Tentec TAPR VNA. From 2005 to 2007, several small-scale new companies (Array Solutions, Mini Radio Solutions, and OMICRON Lab) produced USB-based devices with a maximum operating frequency of 180 MHz. The main reason was that there were no commercial high-frequency MMIC synthesizer chips on the market at that time (although commercial power detection chips had reached several GHz at that time, such as AD8302 gain & phase detector up to 2.7 GHz released in 2001). Later, with the increase in the operating frequency of MMIC synthesizer chip products (up to 4.4 GHz) in the market, from 2008 to 2012, more and more established and emerging companies actively involved in the RF/microwave instrument business, such as National Instruments, Copper Mountain Technologies, AEA Technology Inc, Quonset Microwave, Protek Instrument Co., Ltd, LA Techniques Ltd, Triarchy Technologies, Vaunix Technology, Aaronia AG, RF Explorer, DEEPACE, Windfreak Technology, Signal Hound.

Hence, the evolution of the RF/microwave test equipment is directly affected by the development and demand of communication technology, such as specifications, built-in functions, prices, sizes, and control or operation methods of the test instruments. This chapter surveys and reviews in detail the release of new test instrument products, the participation of new company's in the test instrument business, the test instrument business model, prices, specifications, and test instrument control/operation in the past two decades.

RF/MICROWAVE INSTRUMENTS EVOLUTION

USB-Based Signal Generator

As known that the RF/microwave tester is an essential tool for the design, testing, and installation of those IoT devices. More than ten years ago, RF test instruments up to a few GHz are normally commercialized by several established manufacturers, such as Keysight Technologies (formerly Agilent Technologies), Anritsu, Rohde Schwarz, and Advantest. Although the performance of the commercial test equipment has reached a professional level, those test devices are bulkiness, complex, and have to pay an extremely high cost (typically more than 10,000 US dollars).

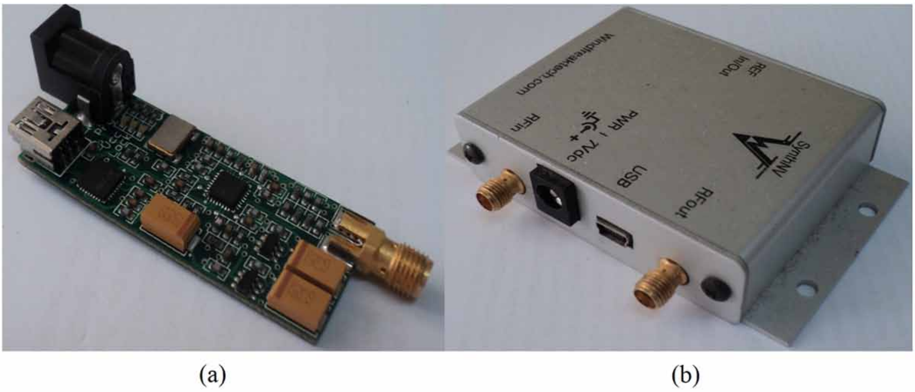
Therefore, former RF/microwave communication amateurs, enthusiasts, or general technicians rarely have their own RF/microwave testers or instruments, such as signal generators, power meters, frequency counters, spectrum analyzers, and vector network analyzer. In addition, many manufacturers with little communication technology development experience dare not participate in the development of such test devices, because this requires a lot of capital and talent in the field, and the market is small.

However, in the past ten years, some new manufacturers and some enthusiasts (own sales) have begun to develop small, USB-based, and low-cost RF instrument products up to a few GHz. This phenomenon is due to the existing affordable monolithic microwave integrated circuits (MMIC) on the open market. At that time, generally, those MMICs are produced by several companies, such as MiniCircuits, Analog Devices/Linear Technology, and Texas Instruments. There are also several emerging manufacturers, such as Qorvo, Broadcom, Microchip, and MACOM, producing MMIC for more specific and high-performance telecommunication applications. Recently, according to business marketing report (Dozier, 2019), the monolithic microwave integrated circuit (MMIC) market value was USD 763.8 million in 2018 year, and it is expected to reach USD 17.41 billion by 2025.

For instance, Analog Devices Inc. produced the ADF4350 synthesizer chip with frequencies up to 4.4 GHz in 2008 (Improved version ADF4351). In the following three and four years, several manufacturers have been used the chip to create relatively cost-effective (priced under 1000 US dollars) USB-based RF signal sources up to 4.4 GHz (manufactured by Windfreak Technologies, Quonset Microwave, etc) as shown in Figure 1, which brought communications amateurs, enthusiasts, and researchers good news and a great surprise.

At the same time, around 2008 and 2009, the term IoT began to be mentioned in academia and industry sectors. Besides, the implementation of the Fourth Industrial Revolution (Industry 4.0) in 2016 and the most recent 5G at the end of 2018, those protocols and regulations are required a lot of wireless communication technologies to support. Indirectly, this has led to the demand and rapid development of low-cost test devices. Therefore, the operating frequencies of released RF/Microwave chips are increasing, such as signal source: AD9361 transceiver module from 70 MHz to 6 GHz (in 2010), MAX2870 frequency synthesizer provided 23 MHz to 6 GHz (in 2012), ADF4355 synthesizer chip up to 6.6 GHz (in 2015), ADF5355 with 13.6 GHz (in 2017), LMX2594 with 15 GHz (in 2017), LMX2595 with 20 GHz (in 2018), ADF4371 from 62.5MHz to 32 GHz (in 2019), and LMX2820 up to 22.6 GHz (in 2020).

Figure 1. (a) First generation SynthUSB low-cost RF signal generator. (b) SynthNV 34MHz – 4.4GHz RF signal generator with power detector



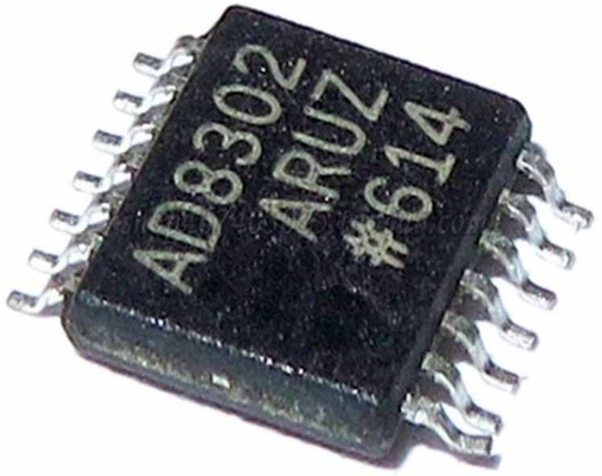
Nowadays, there are many DIY or unbranded USB-based 4.4 GHz signal generators that cost less than 100 US dollars. By using the LMX2595 chip, the recent amateur signal generator has reached up to 20 GHz and the price is less than 400 US dollars. Most RF/microwave chips or components are traded in U.S. dollars. In addition, the currency exchange rates of most countries, especially Asian countries/regions, are lower than the U.S. dollar. Hence, most enthusiasts have a budget of only 50 USD to 400 USD in purchasing RF/microwave amateur instruments.

Power Detector/Diode/Sensor

Power detectors can be separated into two groups, namely passive and active power detectors. Passive power detectors are usually only able to detect a minimum power around –30 dBm, so support with an amplifier is required before a low -power signal is detected by the detector. Furthermore, most passive detectors have a relatively large size and are more expensive than active detectors due to material and hardware machining. Nowadays, most active power detectors (in chip form) are used in amateur devices due to their wide dynamic range, small size, broadband, square-law detector characteristics, and relatively low cost, such as AD8361 (100 kHz to 2.5 GHz), AD8362 (50 Hz to 3.8 GHz), AD8318 (1 MHz to 8 GHz), AD8317/AD8319 (1 MHz to 10 GHz).

Usually, most power detectors are used for amplitude measurement. In the market it is rare to find power detectors up to GHz that are used for phase measurement. AD8302 is the first active power detector released in 2001 that is able to measure amplitude and phase power simultaneously up to 2.7 GHz as shown in Figure 2. The measurement outputs from the AD8302 detector are interpreted in DC voltages (V_{mag} and V_{phase}). The calibration scale between the output V_{mag} (in Volt) from the detector and the actual magnitude reflection coefficient, $\log_{10}|S_{11m\_DUT}|$ (in dB) of the DUT is shown in Figure 3 (a).

Figure 2. AD8302 gain and phase detector chip



Based on the Figure 3 (a), the relationship between V_{mag} (Volt) and of $|S_{11m\_DUT}|$ (linear magnitude) can be represented as:

$$\left|S_{11m\_DUT}\right| = 10^{\frac{\gamma}{20}} \tag{1}$$

For ($0 < V_{mag} \leq 0.9$) V case, the γ in (1) is written as:

$$\gamma = \alpha_6 V_{mag}^6 + \alpha_5 V_{mag}^5 + \alpha_4 V_{mag}^4 + \alpha_3 V_{mag}^3 + \alpha_2 V_{mag}^2 + \alpha_1 V_{mag} + \alpha_o \tag{2}$$

where the polynomial coefficients are given as:

α_o=-42.4726367464274 dB,

α_1=211.943203401082 dB/V,

α_2=-1019.05702655087 dB/V^2,

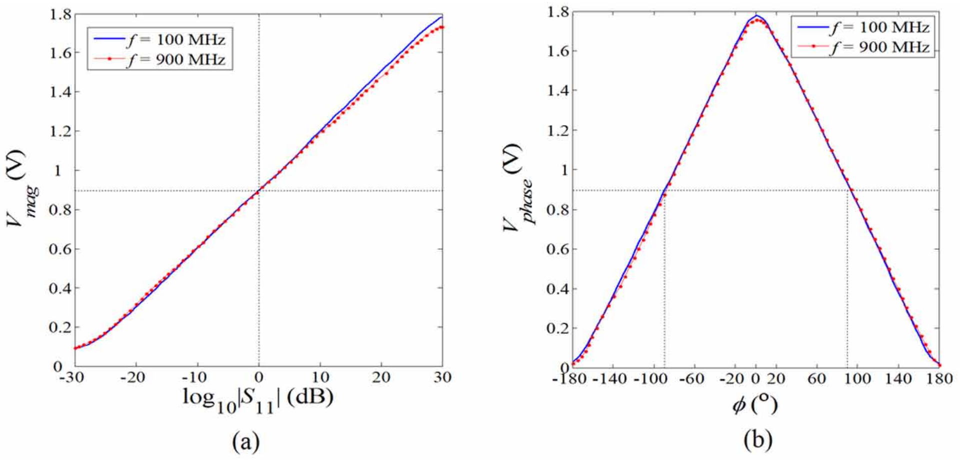
α_3=2939.23929989415 dB/V^3,

α_4=- 4518.67035034208 dB/V^4,

α_5=3520.06111721046 dB/V^5,

α_6=-1090.14798397968 dB/V^6

Figure 3. The transfer characteristics of AD8302 detector: (a) Magnitude, log10|S_{11m_DUT}| and (b) phase shift, ϕ.



while, for (0.9 < V_{mag} ≤ 1.8) V, the γ can be represented in linear equation:

$$\gamma = 33.8994V_{mag} - 30.417257 \tag{3}$$

On the other hand, the V_{phase} (Volt) can be converted to phase shift, ϕ (degree) using expression as:

$$\phi = \beta_5 V_{phase}^5 + \beta_4 V_{phase}^4 + \beta_3 V_{phase}^3 + \beta_2 V_{phase}^2 + \beta_1 V_{phase} + \beta_o \tag{4}$$

where the polynomial coefficients in (4) for (0 < V_{phase} ≤ 0.9) V, are given as:

β_o=182.506874795524 °,

β_1=-210.216183277092 °/V,

β_2=601.763368273347 °/V^2,

β_3=-1314.42197688581 °/V^3,

β_4=1299.16432458607 °/V^4,

β_5=-476.77903380751 °/V^5

On the other hand, for (0.9 < V_{phase} ≤ 1.8) V case, the polynomial coefficients are given as:

β_o=1630.608202309291 °,

β_1= -6.003.830135622119 °/V,

β_2= 9510.346167872143°/V^2,

β_3=-7570.708041938438 °/V^3,

β_4= 2982.427156649023 °/V^4,

β_5=-465.4403049471512 °/V^5

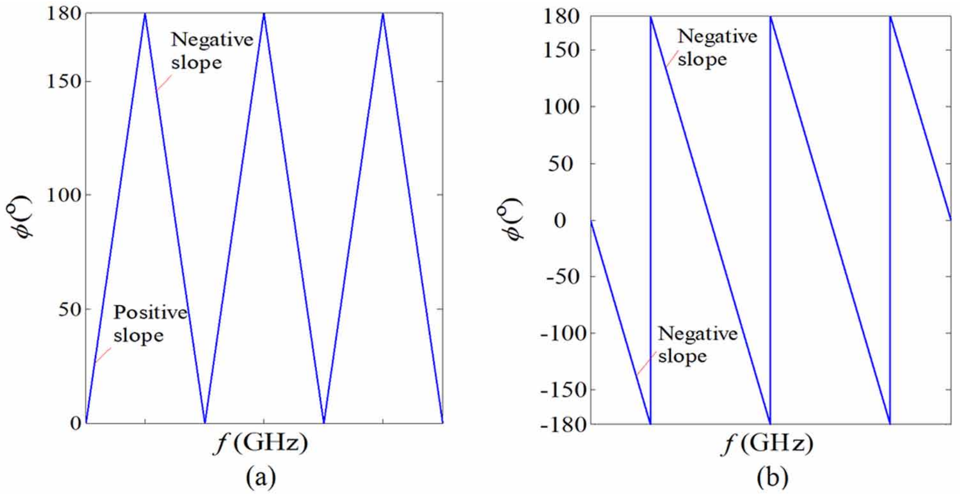
However, based on the phase characteristic in Figure 3 (b), there is an inherent ambiguity of the phase shift, ϕ, since there is no distinction between positive and negative phase shifts (in Figure 4 (a)). In fact, under regular operation, the phase shift, ϕ must always in negative slope. This means that the phase shift must always be decreased to minimum –180° and repeated shift to maximum +180° again when the operating frequencies are sweeping from low to high. To solve the ambiguity of the phase shift, ϕ, an algorithm is developed to compare one phase data point, n to the next phase point (n+1) at a given frequency, f. If the phase shift, ϕ_n+1 of the next frequency is greater than the phase shift, ϕ_n of the current frequency, the negative sign is assigned to the current phase, ϕ_n and vice versa (You *et al.*, 2017):

If $\phi_{n+1} - \phi_n > 0$, Ouput: $-\phi_n$

else $\phi_{n+1} - \phi_n < 0$, Ouput: $+\phi_n$

Finally, the phase shift, ϕ will always exchange between –180° to +180° when the operating frequencies are sweeping as shown in Figure 4 (b).

Figure 4. (a) Absolute and (b) practice phase shift across operating frequency (You et al., 2017)



Vector Network Analyzer

Vector network analyzer (VNA) is a vector instrument used for performance testing, RF system design, and troubleshooting of high-frequency communication equipment. In the past to date, robust and professional VNAs usually commercialized by several established manufacturers, such as Keysight Technologies (formerly Agilent Technologies, Hewlett Packard), Anritsu, Rohde Schwarz, and Advantest. In the past two decades, due to the high cost of the instrument (usually more than US$10,000), bulkiness, and complexity, VNAs are unlikely to be widely used among communication engineers or technicians.

Starting in 2010, some professional and robust VNAs are more likely to be built in the form of the open industry standard PXI (PCI eXtensions for instrumentation) by National Instruments (NI) and Keysight Technologies. The PXI VNA will benefit from the cost, performance, space and flexibility of the latest PC technology. In addition, the PXI function allows the VNA to be integrated with other test and automation modules in a single chassis. Nevertheless, its performance and price are not much different from the conventional bench-top VNA. Recently, the robust VNA been progressively commercialized by other emerging manufacturers, namely Copper Mountain Technologies, Protek Instrument, Tektronix, PICO Technology, Techwin, TIANDA, GRATTEN, Deviser Instruments, SIGLENT Technologies, TongHui, Transcom Instruments, Ceyear Technologies, and Saluki Technology.

Recently, the high-performance VNAs on the market can reach operating frequencies up to 1.1 THz.

Fortunately, the rapid development of communication technology has created a high demand for test equipment. Therefore, in the past 10 years, many cost-effective professional compact PC-based VNAs have been commercialized by manufacturers such as LA Techniques Ltd, AKELA Inc., MegiQ, Copper Mountain Technologies, Tektronix, PICO Technology, and Transcom Instruments. This is of course a great advantage, because it can reduce the burden on the industry or universities in purchasing test equipment. Generally, PC-based compact VNAs can only operate at frequencies up to 6 GHz or 8 GHz, and their prices range from 3,000 USD to 12,000 USD, depending on the data sampling rate (speed) and performance (dynamic range, and full *S*-Parameter functionality) of the VNA. However, the VNA mentioned above is still very expensive for ordinary radio and microwave enthusiasts, and usually they cannot afford it.

Besides professional PC-based VNA, various amateur PC-based VNAs which cost less than 1000 USD (recent price) are accessible in the market as tabulated in Table 1 (McDermott & Ireland, 2004; Baier, 2007; 2009; Bob Reite, 2019; Phil Salas, 2011; 2020; Steber, 2020). After all, the most popular RF/microwave test device in 2020 is the NanoVNA v2, a 3 GHz portable vector network analyzer (VNA) that costs less than 100 US dollars (Phil Salas, 2020; Steber, 2020). In the middle of the end of 2020, the NanoVNA v2 plus4 is upgraded to 4 GHz at a slightly higher price (~130 to 200 USD). For example, the xaVNA up to 3.5 GHz released in 2018, NanoVNA v2 clone, and NanoVNA v2 plus4 are shown in Figure 5. At the end of 2020, ARINST VNA-PR1 from 1 MHz to 6.2 GHz is released at the price of less than 550 USD. Recently in April 2021, a full *S*-parameter NanoVNA v3 up to 6 GHz, so-called LibreVNA has been launched at a price of around ~ 400 to 500 USD. After two or three months, ARINST again come out with a VNA-DL model that achieved a frequency of up to 8.8 GHz (not full *S*-parameter) with an attractive price of 370 USD. In late 2021, another NanoVNA model, namely LiteVNA with a maximum of 6.3 GHz is released at a lower price of 100 USD. This is certainly great news, for it can reduce the burden of the small-scale industry or non-profit university regarding the purchase of test instruments. In addition, the VNA with operating frequency up to 6 GHz is sufficiently used for simple 5G wireless device measurements in the sub-6 GHz band. It should be noted that the sub-6 GHz band extended the operating frequency below 5.925 GHz to 7.125 GHz and will increase as needed in the future. Fortunately, at the end of 2021, ADL5960 integrated VNA front-end IC up to 20 GHz has been released, making the amateur VNA up to 20 GHz is expected to exist in the market in the next two years (hope with the price less than 1000 USD).

Previously, the maximum dynamic range of the aforementioned VNAs is approximately 40/50 dB in the GHz range which is less suitable to be used for high precision laboratory research purposes (Professional VNAs are required to have a dynamic range of more than 100 dB). With a few years of experience in building low-cost VNAs, the dynamic range of most VNAs can now reach 80/90 dB at 3 GHz. Despite this, it is significantly economical and convenient to use for the site measurement, simple troubleshooting, and teaching demonstration instrument/tool. Moreover, the introduction of telecommunication technology using this kind of VNA with operating frequency up to 3 GHz/6 GHz is adequate for undergraduate level students and enthusiasts (You *et al.*, 2017). This will provide more opportunities for the students/engineers in understanding the operation of the RF/Microwave instrument. In the past, VNA was considered a powerful, multi-functional, high-end, and complex instrument that required people with relevant professional knowledge to operate it. However, in the future, VNA will be a common instrument like portable multi-meter nowadays. Since there are many demonstrations of using VNA on YouTube and some circuit schematic design of VNA can be found on the website, how to design and use VNA is no longer a problem.

Table 1. Low-cost portable/USB-based vector network analyser (price < 1000 USD)

Manufacturer	Model	Frequency	*S*-Parameter		Chipset	Standalone	Year	Latest Price (USD)
Paul Kiciak	N2PK VNA	50 kHz – 60 MHz	S_{11}	Mag. & pha.	AD9851	No	2003	~ 260
			S_{21}	Mag. & pha.				
TAPR	Ten-Tec 6000	0.2 – 120 MHz	S_{11}	Mag. & pha.	AD9854 AD8302	No	2005	~ 655
			S_{21}	Mag. & pha.				
VNWA	DG8SAQ VNWA 3v	1 kHz– 1.3 GHz	S_{11}	Mag. & pha.	AD9859	No	2008	~ 450
			S_{21}	Mag. & pha.				
	DG8SAQ VNWA 3SE		S_{11}	Mag. & pha.		No	2017	~ 645
			S_{21}	Mag. & pha.				
			S_{12}	Mag. & pha.				
			S_{22}	Mag. & pha.				

Continued on following page

Table 1. Continued

Manufacturer	Model	Frequency	*S*-Parameter		Chipset	Standalone	Year	Latest Price (USD)
Array Solutions	VNA2180	5 kHz – 180 MHz	S_{11}	Mag. & pha.	AD9859 SA612A	No	2011	~ 1000
			S_{21}	Mag. & pha.				
DEEPACE (KeChuang)	KC901H	100 kHz – 3 GHz	S_{11}	Mag.	HMC830L-P6GE AD8307	Yes	2012	~ 800 (No longer in production)
			S_{21}	Mag.				
Mini Radio Solutions (mRS)	miniVNA	0.1 – 180 MHz	S_{11}	Mag. & pha.	AD8302 AD9951	No	2007	~ 315 (No longer in production)
			S_{21}	Mag. & pha.				
	miniVNA Pro	0.1 – 230 MHz	S_{11}	Mag. & pha.	AD9958	No	2011	~ 450
			S_{21}	Mag. & pha.				
	miniVNA Tiny	1 MHz – 3 GHz	S_{11}	Mag. & pha.	ADF4350	No	2014	~ 500
			S_{21}	Mag. & pha.				
PocketVNA	Pocket VNA	500 kHz –4 GHz	S_{11}	Mag. & pha.	AD7392	No	2016	~ 490
			S_{21}	Mag. & pha.				
			S_{12}	Mag. & pha.				
			S_{22}	Mag. & pha.				
Michael Wurm	AnnaLyza VNA	2.2 GHz–2.7 GHz	S_{11}	Mag. & pha.	-	No	2018	~400 (No longer in production)
			S_{21}	Mag. & pha.				
			S_{12}	Mag. & pha.				
			S_{22}	Mag. & pha.				
Red Pitaya	VNA module STEMlab board	500 kHz–62 MHz	S_{11}	Mag. & pha.	-	No	2018	~350
xaxaxa Development	xaVNA	137 MHz–3.5GHz	S_{11}	Mag. & pha.	ADF4350	No	2018	~275
			S_{21}	Mag. & pha.				

Continued on following page

Table 1. Continued

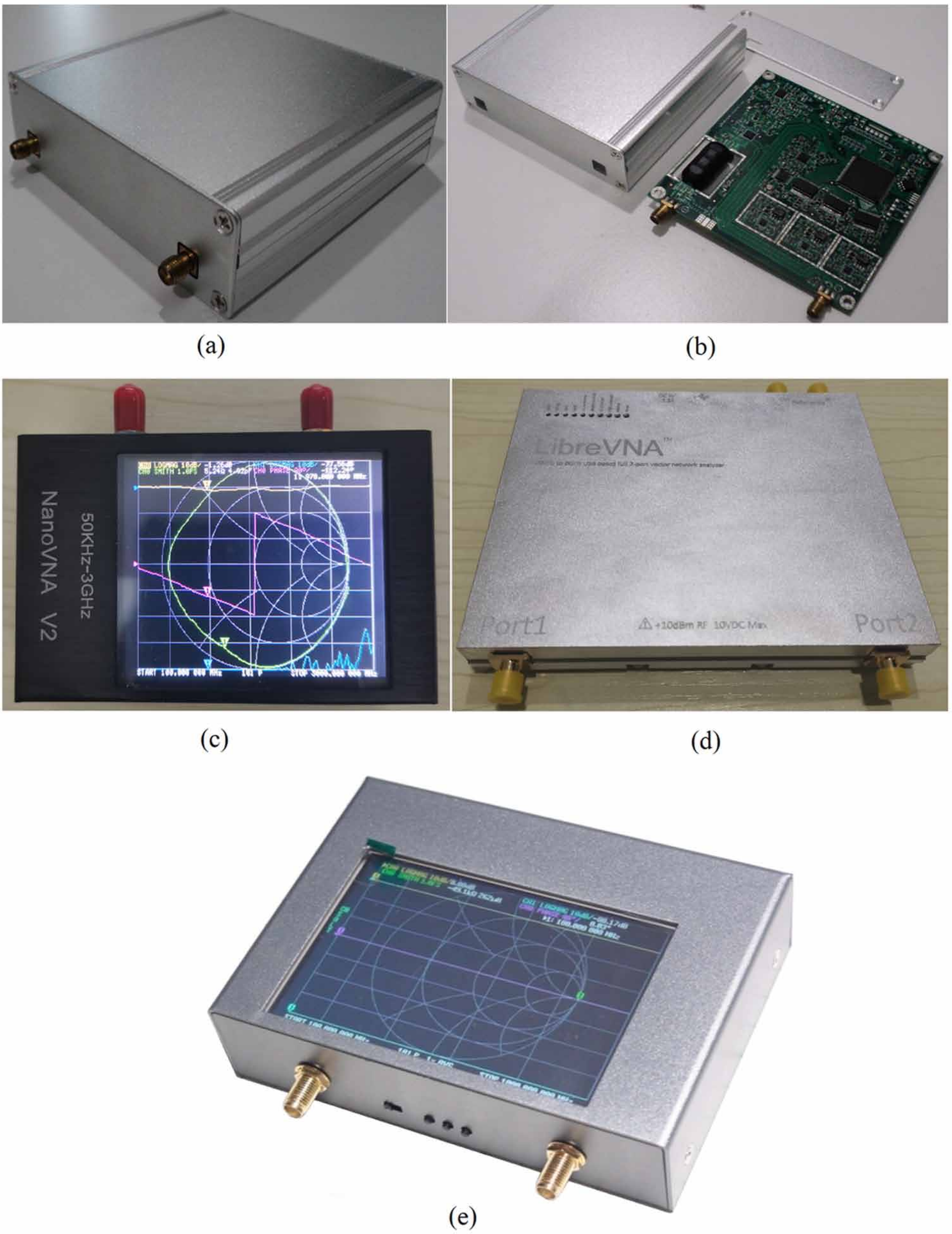
Manufacturer	Model	Frequency	*S*-Parameter		Chipset	Standalone	Year	Latest Price (USD)
ARINST	VR 23- 6200	23 MHz–6.2 GHz	S_{11}	Mag. & pha.	-	Yes	2018	~260
	VR 1- 6200	1 MHz–6.2 GHz	S_{11}	Mag. & pha.	-	Yes	2019	~410
	VNA-PR1	1 MHz – 6.2 GHz	S_{11}	Mag. & pha.	-	Yes	2020	~540
			S_{21}	Mag. & pha.				
	VNA-DL	1 MHz – 8.8 GHz	S_{11}	Mag. & pha.	-	No	2021	~350
			S_{21}	Mag. & pha.				
Tomohira AKA Edy555	NanoVNA	50 kHz– 300 MHz	S_{11}	Mag. & pha.	Si5351A	Yes	2017	~50 (No longer in production)
			S_{21}	Mag. & pha.				
Digital Signal Technology	DZV-1	100 kHz–500 MHz	S_{11}	Mag. & pha.	-	No	2017	~500
			S_{21}	Mag. & pha.				
			S_{12}	Mag. & pha.				
			S_{22}	Mag. & pha.				
Hugen79	NanoVNA-H	50 kH – 900 MHz	S_{11}	Mag. & pha.	Si5351	Yes	2019	~45 (No longer in production)
			S_{21}	Mag. & pha.				
	NanoVNA-H 4	50 kHz – 1.5 GHz	S_{11}	Mag. & pha.	Si5351	Yes		~ 80
			S_{21}	Mag. & pha.				
BH5HNU	NanoVNA-F	50 kHz – 1 GHz	S_{11}	Mag. & pha.	Si5351	Yes	2019	~100 (No longer in production)
			S_{21}	Mag. & pha.				
		10 kHz –1.5 GHz	S_{11}	Mag. & pha.	Si5351	Yes	Late 2019	~100
			S_{21}	Mag. & pha.				

Continued on following page

Table 1. Continued

Manufacturer	Model	Frequency	*S*-Parameter		Chipset	Standalone	Year	Latest Price (USD)
HCXQS & OwOComm	NanoVNA v2	50 kHz – 3 GHz	S_{11}	Mag. & pha.	Si5351 ADF4350 AD8342	Yes	2020	~50 to 60
			S_{21}	Mag. & pha.				
	NanoVNA V2 Plus4	50 kHz – 4 GHz	S_{11}	Mag. & pha.	Si5351 ADF4350 AD8342	Yes	Late 2020	~ 130 to 200
			S_{21}	Mag. & pha.				
jankae	LibreVNA	100 kHz – 6 GHz	S_{11}	Mag. & pha.	Si5351C MAX2871 ADL5801 LT5560	No	2021	~ 400 to 500
			S_{21}	Mag. & pha.				
			S_{12}	Mag. & pha.				
			S_{22}	Mag. & pha.				
Hugen79	LiteVNA	50 kHz – 6.3 GHz	S_{11}	Mag. & pha.	-	Yes	Late 2021	~ 100 to 130
			S_{21}	Mag. & pha.				

Figure 5. (a) xaVNA released in 2018. (b) The xaVNA's circuit board. (c) NanoVNA v2 clone available in the market in 2020. (d) LibreVNA launched in 2021. (e) NanoVNA v2 plus4 up to 4 GHz released in 2020

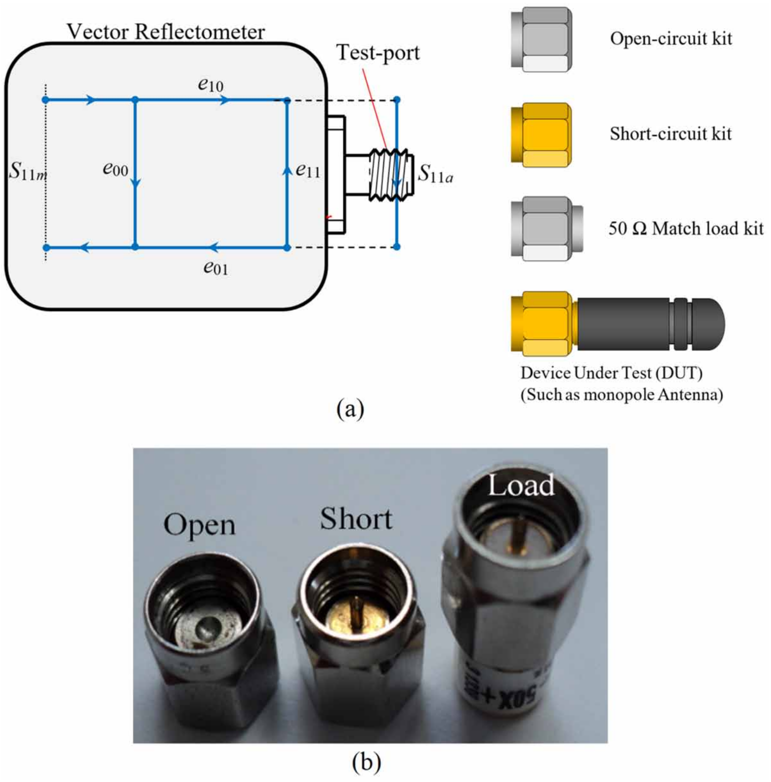


One-Port VNA Calibration

The systematic errors existed in the vector reflectometer can be represented by one-port three-term error network model as shown in Figure 6. The three errors of e_{00}, e_{11}, and $e_{10}e_{01}$ are resulted by imperfect directivity, source mismatch, and transmission loss or reflection tracking, respectively (Rytting, 2001). Based on the network model, the relationship between the measured reflection coefficient, S_{11m} and the calibrated reflection coefficient, S_{11a} of the device under test (DUT) at test-port is given as:

$$S_{11a} = \frac{S_{11m} - e_{11}}{e_{22}S_{11m} + \left(e_{12}e_{21} - e_{11}e_{22}\right)} \tag{5}$$

Figure 6. (a) Error network for the one-port vector reflectometer and (b) three calibration kits (Open, short and 50 Ω load)



The three unknown complex coefficients (e_{00}, e_{11}, and e_{10} e_{01}) values in (5) can be found using three calibration kits, namely open-circuit, short-circuit, and 50 Ω match load. The open-circuit, short-circuit, and 50 Ω match load are respectively connected to test-port and its reflection coefficients, $S_{11m—o}$, S_{11m_s}, and S_{11m_l} are measured. Finally, the e_{00}, e_{11}, and e_{10} e_{01} are calculated as:

$$e_{00} = \frac{S_{11a\_s}S_{11a\_l}S_{11m\_o}\Delta_{l\_s} + S_{11a\_o}S_{11a\_s}S_{11m\_l}\Delta_{s\_o} + S_{11a\_o}S_{11a\_m}S_{11m\_s}\Delta_{o\_l}}{D} \tag{6a}$$

$$e_{11} = \frac{-\left(S_{11a\_o}\Delta_{l\_s} + S_{11a\_l}\Delta_{s\_o} + S_{11a\_s}\Delta_{o\_l}\right)}{D} \tag{6b}$$

$$e_{10}e_{01} - e_{00}e_{11} = \frac{S_{11a\_o}S_{11m\_o}\Delta_{l\_s} + S_{11a\_l}S_{11m\_l}\Delta_{s\_o} + S_{11a\_s}S_{11m\_s}\Delta_{o\_l}}{D} \tag{6c}$$

where

$$\Delta_{o\_l} = S_{11m\_o} - S_{11m\_l},\ \Delta_{s\_o} = S_{11m\_s} - S_{11m\_o}, \text{ and } \Delta_{l\_s} = S_{11m\_l} - S_{11m\_s}$$

The denominator, D in (6a), (6b), and (6c) is given as:

$$D = S_{11a\_l}S_{11a\_s}\Delta_{l\_s} + S_{11a\_o}S_{11a\_s}\Delta_{s\_o} + S_{11a\_l}S_{11a\_o}\Delta_{a\_l}$$

The S_{11a_o}, S_{11a_s}, and S_{11a_l} represents the known calibrated reflection coefficients for the open, short, and match-load standards as tabulated in Table 2.

In most amateur VNAs, users are allowed to use either ideal values or practical values in the calibration process. Usually, at low operating frequency (< 3 GHz), the fringing effect for open-circuit on the test-port is not very significant, so the ideal value ($S_{11m\_o} = 1+j\,0$) can be used. For short-circuit cases, the ideal value ($S_{11m\_s} = -1 + j\,0$) is only suitable for flush short-circuit kits (not accurate for short-circuit offset kits). On the other hand, the quality of match-load kits is highly dependent on the absorption material used and the precision of kit machining. Usually, for brander and expensive calibration kits, the manufacturer will supply parameter values for the kits, such as C_o, C_1, C_2, C_3, L_o, L_1, L_2, L_3, offset delay, and loss. In fact, in today's market, there are many options for the low-cost calibration kits as shown in Figure 6 (b). Some termination kits (up to 6 GHz) cost less than 2 USD. However, normally, parameter values are not supplied for such low-cost kits.

If the user does not know the parameters for the calibration kits, then the ideal values have to be used in the calibration (assume all the kits are ideal and perfect) and error calculation of (6a) (6b), and (6c) can be simplified as:

$$e_{00} = S_{11m\_l} \tag{7a}$$

$$e_{11} = \frac{S_{11m\_o} + S_{11m\_s} - 2S_{11m\_l}}{D_1} \tag{7a}$$

$$e_{10}e_{01} - e_{00}e_{11} = \frac{S_{11m\_o}S_{11m\_1} + S_{11m\_s}S_{11m\_l} - 2S_{11m\_o}S_{11m\_s}}{D_1} \tag{7c}$$

The denominator, D_1 in (7a), (7b), and (7c) is given as:

$$D_1 = S_{11m\_s} - S_{11m\_o}$$

Table 2. Standard calibration values of S_{11a_o}, S_{11a_s}, and S_{11a_l} (You et al., 2017; You, 2017)

Calibration Kit	Ideal	Practical
Open-circuit	$S_{11a\_o} = 1 + j0$	$S_{11a\_o} = \frac{1-\tilde{Y}_a}{1+\tilde{Y}_a}$ $= \frac{1 - j\left(\omega/Y_o\right)\left(C_o + C_1 f + C_2 f^2 + C_3 f^3\right)}{1 + j\left(\omega/Y_o\right)\left(C_o + C_1 f + C_2 f^2 + C_3 f^3\right)}$ Offset delay (in unit ps) and the loss (in unit GΩ /s) of the open-circuit kit.
Short-circuit	$S_{11a\_o} = -1 + j0$	$S_{11a\_S} = \frac{\tilde{Z}_a - 1}{\tilde{Z}_a + 1}$ $= \frac{j\left(\omega/Z_o\right)\left(L_o + L_1 f + L_2 f^2 + L_3 f^3\right) - 1}{j\left(\omega/Z_o\right)\left(L_o + L_1 f + L_2 f^2 + L_3 f^3\right) + 1}$ Offset delay (in unit ps) and the loss (in unit GΩ /s) of the short-circuit kit.
50 Ω match-load	$S_{11a\_l} = 0 + j0$	$S_{11a\_l} \approx 0 + j0$ (Depend on the used absorption material and the precision of kit machining)

Two-Port VNA Calibration (Open-Short-Load-Thru)

Before the actual measurement of the device under test (DUT), the test port 1 and port 2 of the two-port VNA need to be calibrated. For simple analysis, the complex two-port error network model is usually divided into forward error network and reverse error network, as shown in Figures 7(a) and 7(b). Based on the error network, the calibration equation of the full scattering parameters (*S*-parameter) is given as (Rytting, 2001):

$$S_{11a} = \frac{\left(\frac{S_{11m} - e_{00}}{e_{10}e_{01}}\right)\left[1 + \left(\frac{S_{22m} - e_{33}}{e_{23}e'_{32}}\right)e'_{22}\right] - e_{22}\left(\frac{S_{21m} - e_{30}}{e_{10}e_{32}}\right)\left(\frac{S_{12m} - e_{03}}{e_{23}e'_{01}}\right)}{D_2} \tag{8a}$$

$$S_{21a} = \frac{\left(\frac{S_{21m} - e_{30}}{e_{10}e_{32}}\right)\left[1 + \left(\frac{S_{22m} - e_{33}}{e_{23}e'_{32}}\right)\left(e'_{22} - e_{22}\right)\right]}{D_2} \tag{8b}$$

$$S_{22a} = \frac{\left(\frac{S_{22m} - e_{33}}{e_{23}e'_{32}}\right)\left[1 + \left(\frac{S_{11m} - e_{00}}{e_{10}e_{01}}\right)e_{11}\right] - e'_{11}\left(\frac{S_{21m} - e_{30}}{e_{10}e_{32}}\right)\left(\frac{S_{12m} - e_{03}}{e_{23}e'_{01}}\right)}{D_2} \tag{8c}$$

$$S_{12a} = \frac{\left(\frac{S_{12m} - e_{03}}{e'_{23}e'_{01}}\right)\left[1 + \left(\frac{S_{11m} - e_{00}}{e_{10}e_{01}}\right)\left(e_{11} - e'_{11}\right)\right]}{D_2} \tag{8d}$$

where denominator, D_2 in (8a), (8b), (8c), and (8d) is given as:

$$D_2 = \left[1 + \left(\frac{S_{11m} - e_{00}}{e_{10}e_{01}}\right)e_{11}\right]\left[1 + \left(\frac{S_{22m} - e_{33}}{e_{23}e'_{32}}\right)e'_{22}\right] - \left(\frac{S_{21m} - e_{30}}{e_{10}e_{32}}\right)\left(\frac{S_{12m} - e_{03}}{e_{23}e'_{01}}\right)e_{22}e'_{11}$$

All the unknown complex value of the error terms in Equation (8) are defined in Table 3.

Table 3. Error terms definition for forward and reverse error networks

Error Type	Forward Error Network		Reverse Error Network	
	Port 1	Port 2	Port 1	Port 2
Directivity	e_{00}	-	e_{33}	-
Source Mismatch	e_{11}	e_{22}	e'_{11}	e'_{22}
Reflection Tracking	$e_{10}e_{01}$	-	$e_{23}e'_{32}$	-
Transmission Tracking	-	$e_{10}e_{32}$	-	$e_{23}e'_{01}$
Leakage	-	e_{30}	-	e_{03}

Most amateur VNAs can only measure reflection coefficient, S_{11m} and transmission coefficient, S_{21m} (not a full *S*-parameter VNA) to reduce construction costs and make

VNAs affordable for more enthusiasts (Henze, *et al.*, 2014). Therefore, S_{22m} and S_{12m} in (8a) cannot be measured by this kind of VNA, and only the forward error network (half error network), as shown in Figure 7(a) is considered in the calibration. In this process, the reflection coefficient, S_{11a} of port 1 is calibrated using the same procedure as described in the 'One-Port VNA Calibration' section and the e_{00}, $e_{10}e_{01}$, and e_{11} in Figure 7(a) are solved.

In fact, the calibration equation (8b) of the transmission coefficient, S_{21a} at port 2 has 9 error terms that need to be solved, namely e_{30}, e_{03}, e_{33}, e_{22}, $e_{10}e_{32}$, $e_{23}e'_{32}$, e'_{22}, $e_{23}e'_{01}$, and e'_{11}. To simplify the mathematical calculations [based on Figure 7 (a)], only 6 error terms (e_{00}, $e_{10}e_{01}$, e_{11}, e_{30}, e_{22}, and $e_{10}e_{32}$) are involved in this two-port calibration calculation, so-called transmission response technique. The first 3 terms of e_{00}, $e_{10}e_{01}$, and e_{11} in (8b) are determined in reflection coefficient, S_{11a} calibration using open-circuit, short-circuit, and 50 Ω matched load kits. On the other hand, the remaining 3 terms (e_{30}, e_{22}, and $e_{10}e_{32}$) are solved as:

$$e_{30} = S_{21m\_l} \tag{9a}$$

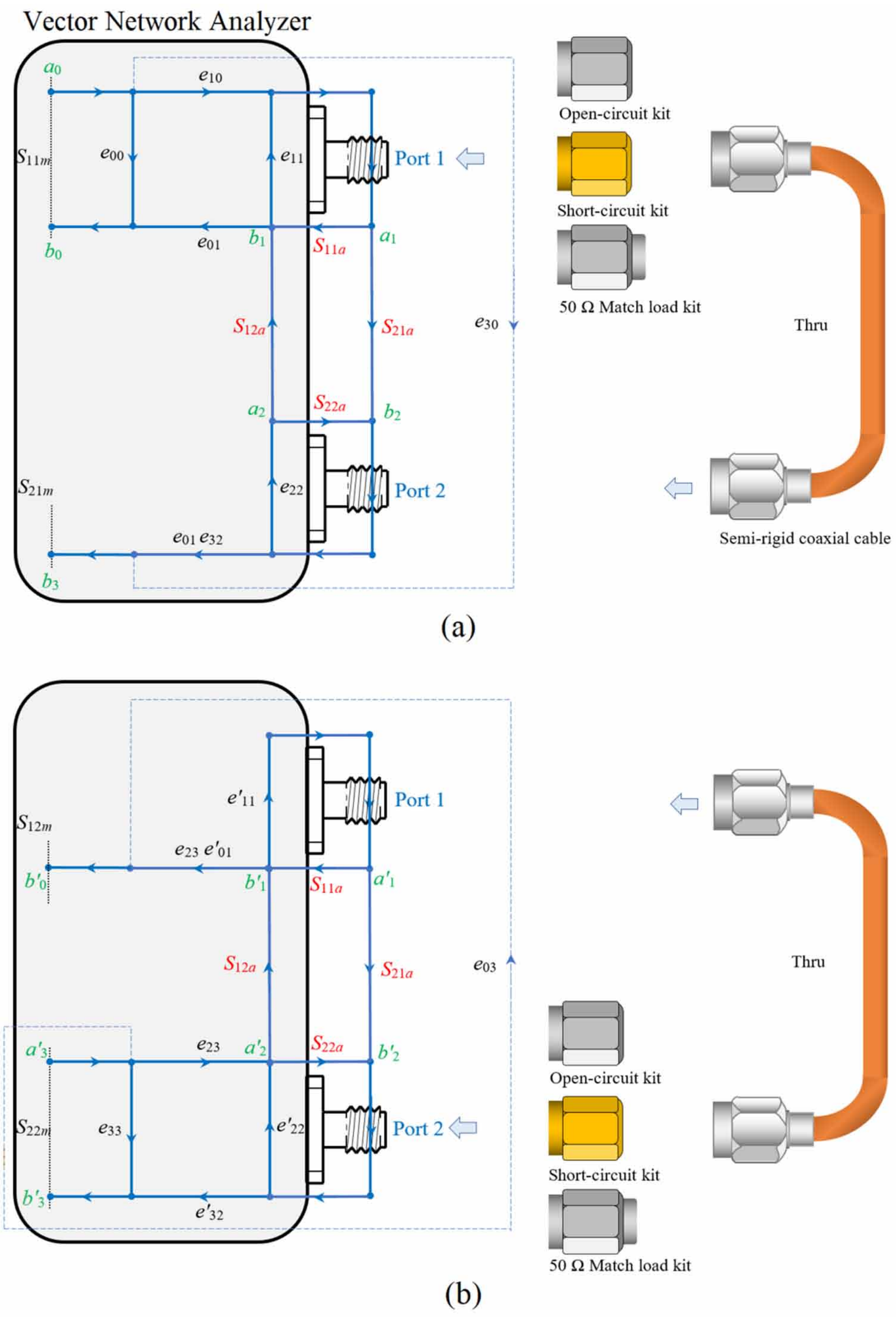
$$e_{22} = \frac{S_{11m\_T} - e_{00}}{e_{11}S_{11m\_T} - \left(e_{00}e_{11} - e_{01}e_{10}\right)} \tag{9b}$$

$$e_{10}e_{32} = \left(S_{21m\_T} - e_{30}\right)\left(1 - e_{11}e_{22}\right) \tag{9c}$$

where S_{21m_l} is the transmission coefficient measured at port 2 when both port 1 and port 2 are respectively connected to 50 Ω matched load kits. The S_{11m_T} and S_{21m_T} are the reflection coefficient measured at port 1 and the transmission coefficient measured at port 2 when port 1 and port 2 are connected using a coaxial cable. The other error terms at port 1 and port 2 for reverse error network are treated as zero values (e_{33} » e_{03} » e'_{22} » $e_{23}e'_{32}$ » e'_{22}, $e_{23}e'_{01}$ » e'_{11} » 0). Finally, the simplified of (8b) can be written as:

$$S_{21a} = \frac{\left(\dfrac{S_{21m} - e_{30}}{e_{10}e_{32}}\right)}{1 + \left(\dfrac{S_{11m} - e_{00}}{e_{10}e_{01}}\right)e_{11}} \tag{10}$$

Figure 7. (a) Forward and (b) reverse error network models (6 error terms of forward + 6 error terms of reverse = 12 error terms)



Two-Port VNA Calibration (Thru-Reflect-Line)

Thru-Reflect-Line (TRL) calibration technique is another full *S*-parameter calibration method for two-port VNA calibration. TRL assumes that the error network for both ports is symmetry or identical as shown in Figure 8(a). Therefore, TRL has only 8 unknown terms that need to be resolved compared to the rigorous full OSLT calibration techniques (12 unknown error terms). The TRL method is suitable for the coaxial type and non-coaxial type connectors (such as rectangular waveguides), as well as free-space measurement set-up calibration. Based on Equations (8a) to (8d) and the error network in Figure 8 (a), the S_{11a}, S_{21a}, S_{22a}, and S_{12a} are simplified as:

$$S_{11a} = \frac{S_{11m} - e_{00} - S_{21a}S_{12m}\left(\frac{e_{10}e_{22}}{e_{23}}\right)}{e_{11}S_{11m} - \left(e_{00}e_{11} - e_{10}e_{01}\right)} \tag{11a}$$

$$S_{21a} = \frac{S_{21m} - S_{11a}S_{21m}e_{11}}{\left(\frac{e_{22}e_{10}}{e_{23}}\right)S_{22m} - \left[\frac{e_{10}\left(e_{22}e_{33} - e_{32}e_{23}\right)}{e_{23}}\right]} \tag{11b}$$

$$S_{12a} = \frac{\left(\frac{e_{10}}{e_{23}}\right)S_{12m} - S_{22a}S_{12m}\left(\frac{e_{10}e_{22}}{e_{23}}\right)}{e_{11}S_{11m} - \left(e_{00}e_{11} - e_{10}e_{01}\right)} \tag{11c}$$

$$S_{22a} = \frac{\left(\frac{e_{10}}{e_{23}}\right)S_{22m} - S_{12a}S_{21m}e_{11} - \frac{e_{10}e_{33}}{e_{23}}}{\left(\frac{e_{10}e_{22}}{e_{23}}\right)S_{22m} - \left[\frac{e_{10}\left(e_{22}e_{33} - e_{32}e_{23}\right)}{e_{23}}\right]} \tag{11d}$$

In the TRL calibration, the parameters S_{11a}, S_{21a}, S_{22a}, and S_{12a} are considered as known ideal values and the S_{11m}, S_{21m}, S_{22m}, and S_{12m} are the measurement values as tabulated in Table 4. On the other hand, e_{11}, e_{00}, e_{10}, e_{01}, e_{22}, e_{33}, e_{32}, and e_{23} are the unknown error terms that are desired to be determined in the TRL calibration routine.

Table 4. Through, reflection, and line connection in TRL calibration

Connection	Known Ideal Values		Measured Values	
	Port 1	Port 2	Port 1	Port 2
Thru [Figure 8 (b)]	$S_{11a} = 0$ $S_{12a} = 1$	$S_{22a} = 0$ $S_{21a} = 1$	$S_{11m} = S_{11m\_T}$ $S_{12m} = S_{12m\_T}$	$S_{22m} = S_{22m\_T}$ $S_{21m} = S_{21m\_T}$
Reflect [Figure 8 (c)]	$S_{11a} = -1$ $S_{12a} = 0$	$S_{22a} = -1$ $S_{21a} = 0$	$S_{11m} = S_{11m\_S}$ $S_{12m} = S_{12m\_S}$	$S_{22m} = S_{22m\_S}$ $S_{21m} = S_{21m\_S}$
Line [Figure 8 (d)]	$S_{11a} = 0$ $S_{12a} = e^{-j\beta L}$	$S_{22a} = 0$ $S_{21a} = e^{-j\beta L}$	$S_{11m} = S_{11m\_L}$ $S_{12m} = S_{12m\_L}$	$S_{22m} = S_{22m\_L}$ $S_{21m} = S_{21m\_L}$

Insert the values of each case connection (in Table 4) into Equations (11a) to (11d). Hence, for ‘Thru’ connection, the (11a) to (11d) are rewritten as:

$$S_{11m\_T} = e_{00} + ke_{22}S_{12m\_T} \tag{12a}$$

$$kS_{12m\_T} = e_{11}S_{11m\_T} - \Delta_x \tag{12b}$$

$$S_{21m\_T} = ke_{22}S_{22m\_T} - k\Delta_y \tag{12c}$$

$$kS_{22m\_T} = e_{11}S_{21m\_T} + ke_{33} \tag{12d}$$

where $k = \frac{e_{10}}{e_{23}}$, $\Delta_x = e_{00}e_{11} - e_{10}e_{01}$, and $\Delta_x = e_{22}e_{33} - e_{32}e_{23}$. However, only four equations (12a) to (12d) are not sufficient to solve the 8 error terms. Therefore, ‘Reflect’ and ‘Line’ connections are involved in the calibration process (different connection situations). Similarly, for ‘Reflect’ connection, yields

$$S_{11m\_S} = e_{00} - e_{11}S_{11m\_S} + \Delta_x \tag{13a}$$

$$kS_{12m\_S} = -ke_{22}S_{12m\_S} \tag{13b}$$

$$S_{21m\_S} = -e_{11}S_{21m\_S} \tag{13c}$$

$$kS_{22m\_S} = ke_{33} - ke_{22}S_{22m\_S} + k\Delta_y \tag{13d}$$

The physical transmission length, L and propagation constant, β of the delay line used in the 'Line' connection are known values and the equations are given as:

$$S_{11m\_L} = e_{00} + ke_{22}e^{-j\beta L}S_{12m\_L} \tag{14a}$$

$$kS_{12m\_L} = e^{j\beta L}e_{11}S_{11m\_L} + e^{j\beta L}\Delta_x \tag{14b}$$

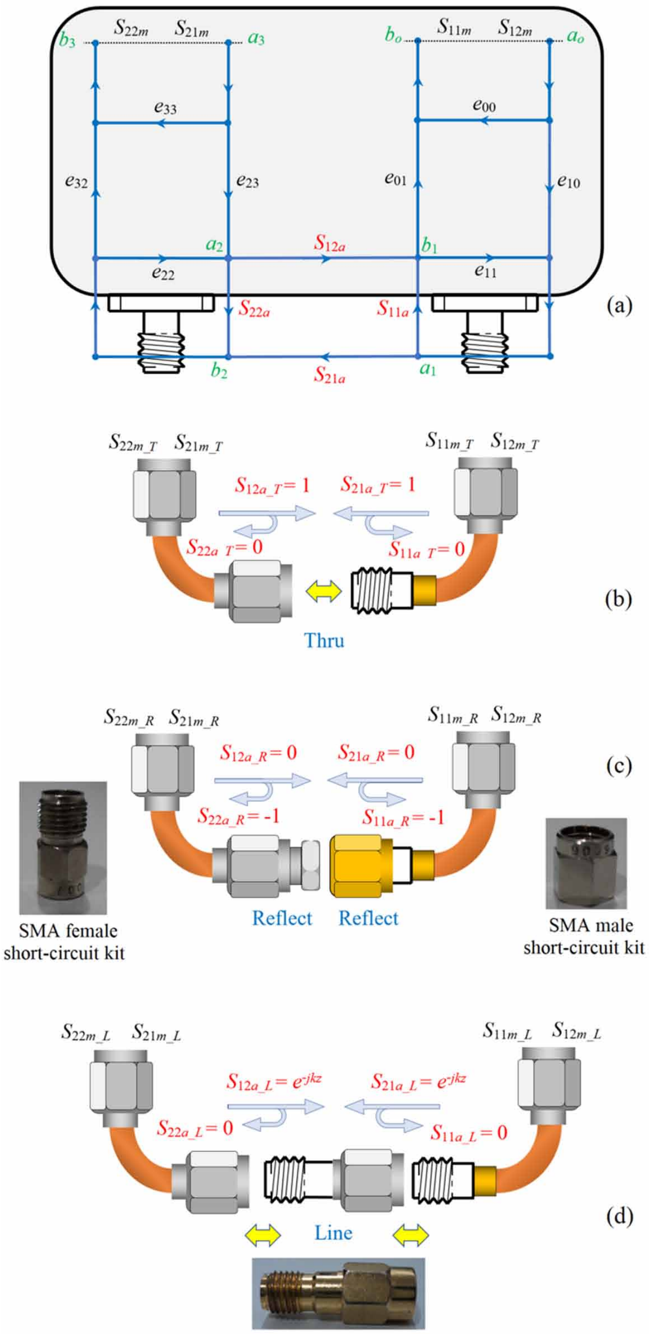
$$S_{21m\_L} = -e^{-j\beta L}ke_{22} \tag{14c}$$

$$kS_{22m\_L} = e_{11}e^{j\beta L}S_{21m\_L} - ke_{33} + k\Delta_y \tag{14d}$$

Finally, 12 linear equations were generated. The 12 sets of linear equations can be expressed as equation (15) in matrix form and solved by numerical methods, such as Cramer's rule (You, 2017).

$$\begin{bmatrix} 1 & 0 & 0 & 0 & S_{12m\_T} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & S_{11m\_T} & -1 & 0 & 0 & 0 & -S_{12m\_T} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & S_{22m\_T} & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & S_{21m\_T} & 0 & 1 & 0 & 0 & -S_{22m\_T} & 0 & 0 & 0 & 0 & 0 \\ 1 & -S_{11m\_S} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -S_{12m\_S} & 0 & -S_{12m\_S} & 0 & 0 & 0 & 0 & 0 \\ 0 & -S_{21m\_S} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -S_{22m\_S} & 1 & -S_{22m\_S} & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & e^{-j\beta L}S_{12m\_L} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{j\beta L}S_{11m\_L} & e^{j\beta L} & 0 & 0 & 0 & -S_{12m\_L} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & & -e^{-j\beta L} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{j\beta L}S_{21m\_L} & 0 & 1 & 0 & 0 & -S_{22m\_L} & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} e_{00} \\ e_{11} \\ \Delta_x \\ ke_{33} \\ ke_{22} \\ k\Delta_y \\ k \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} S_{11m\_T} \\ 0 \\ S_{21m\_T} \\ 0 \\ S_{11m\_S} \\ 0 \\ S_{21m\_S} \\ 0 \\ S_{11m\_L} \\ 0 \\ S_{21m\_L} \\ 0 \end{bmatrix} \tag{15}$$

Figure 8. (a) Eight-term error network model which errors can eliminate by Thru-Reflect-Line (TRL) calibration. (b) The 'Thru' connection measurement. (c) The 'Reflect' measurement using short-circuit kits. (d) The 'Line' measurement using SMA female to male adapter



Spectrum Analyzer

Besides vector network analyzer (VNA), spectrum analyzer (SA) is another most important instrument particularly in the field of wireless telecommunication (Armitage, 2006; Efrain Santos-Luna *et al.*, 2019). In terms of complexity, VNA is indeed a more complex instrument than SA. As known that VNA consists of a signal generator, but conventional SA does not have a signal generator and only measures received external signals (normally wireless signals) over frequencies (sweep measurement with high sampling rate). Recently, some spectrum analyzers are equipped with a tracking generator (with an internal signal generator) that can generate a frequency sweeping signal which the SA can be used as a simple scalar network analyzer (SNA). The difference between the SA and the VNA is described in Table 5.

Nowadays, some simple amateur RF spectrum analyzers up to 4.4 GHz have been sold online such as the LTDZ 35M-4400M spectrum analyzer with 4.3 inch LCD (~ 100 USD). Now, the market also has a tiny size spectrum analyzer up to 900 MHz, namely a TinySA spectrum analyzer with a price of ~50 USD. Many enthusiasts are fond of the spectrum analyzer due to its size and price. Some enthusiasts like the programmable spectrum analyzer, where the spectrum analyzer is built from a software-defined radio (SDRs) (to be discussed in the next section). On the other hand, most technicians (usually from small telecommunications companies) still prefer to use the RF Explorer spectrum analyzer because of its small size and portability, as well as the ability to control and analyze measurement signals through a PC (advanced software interface). In the market, there are also several manufacturers producing cost-effective spectrum analyzers up to 6 GHz (< 700 USD), such as Triarchy Tech. and ARINST.

Table 5. Comparison features between spectrum analyzer (SA) and vector network analyser (VNA)

No.	Spectrum Analyzer (SA)	Vector Network Analyzer (VNA)
1	Contains a receiver. (Some SA contains tracking generator provide effective scalar transmission measurements)	Contains a signal source and receiver.
2	Normally contains one port (single channel).	Normally contains two port or multi-port. (Some VNA contains one port, so-called vector reflectometer)
3	No ratioed measurements. Real power amplitude measurements (Only amplitude without phase).	Ratioed measurements. Vector *S*-parameters measurement, such as complex reflection coefficient and complex transmission coefficient.
4	Measures unknown signals, such as wireless signal.	Uses and measures known stimulus.
5	Limited calibration capability (less precise and accurate).	Offers advanced calibration (more precise and accurate).
6	Can handled analog and digitally modulated signals.	Only handled analog and pulsed signals.
7	Normally use for received signal analysis, such as bandwidth, characterize carrier power, sidebands, harmonics, signal-to-noise ratio, and spurs.	Normally use for RF circuits and antennas characterization or design.
8	Frequency-domain measurements.	Frequency-domain measurements. (Also allow time-domain measurements with built-in Fast-Fourier Transform module)

Software-Defined Radio (SDR)

Nowadays, the development of professional and amateur RF/microwave instruments has tended towards software-defined instruments, so-called software-defined radios (SDRs). This means that most specifications (such as filtering and sub-operating frequency selection) of the developed instrument are determined by the software program instead of hardware. Thus, the use of hardware components can be reduced in the construction of instruments and the functions of those components will be supported by software (using mathematical approaches). This will reduce the size and cost of the instrument, as well as the performance of the instrument, which can be improved due to most signals being digitally processed (Mitola, 1993).

Generally, software-defined radios (SDRs) are built in the form of PC-based circuit modules. The circuit module of the SDR will be connected to the personal computer (PC) via a USB cable and controlled by a software program (packaged with GUI feature). By using the SDR module, many different functions and applications can be reconfigured by changing the software program settings without having to modify or replace the hardware. For instance, the SDR module can be programmed to function as a spectrum analyzer or signal generator or power meter, or radio broadcasting system. In fact, the term 'software-defined radio' was first defined by Stephen Blust in 1995. Later, Federal Communications Commission (FCC) in 2000 proposed SDR as a new equipment category and formally define it as:

A fully software driven and performs all digital signal processing using programmable digital signal processors, general purpose microprocessors, or field programmable gate arrays

Although, software radios already existed in the market in the early 1990s and term of 'software-defined radio (SDR)' was initially mentioned in 1995, but SDR was not so popular at that time. SDRs became popular in the late 2000s due to the fact that by that time many MMICs had started to be commercialized openly and massively in the market as well as the emergence of microprocessor technology. Hence, in 2009, the concept of 'software-defined radio' was comprehensively re-defined by International Telecommunication Union (ITU) as (International Telecommunication Union, 2009):

A radio transmitter and/or receiver employing a technology that allows the RF operating parameters including, but not limited to, frequency range, modulation type, or output power to be set or altered by software, excluding changes to operating parameters which occur during the normal pre-installed and predetermined operation of a radio according to a system specification or standard

Today, many types of amateur SDR (receiver and transceiver) have been commercialized (Gannapathy *et al.*, 2014). The other main reason SDR become popular is the existing supported open-source software, such as GNU Radio. This allows more enthusiasts to be able to afford it (within the budget) and be able to self-learn and develop their own RF instrument. The new enthusiasts and undergraduates will better understand and experience actual signal phenomena through some trial practices using the simple SDR module platform. The learning process will become more interesting and effective when the theory in the classroom or textbook is transformed into real practice.

Traditional Hardware vs. Software-Defined Radio (SDR)

In a traditional receiver, all the actual work of understanding the signal is done by physical components or hardware as illustrated in Figure 9 (a) (Rohde & Schwarz, 2004a; 2004b). In a software-defined radio receiver, the signal is first converted to digital form, and then reloaded by the computer. For instance, the SDR-based transceiver (combination of the transmitter and receiver in single circuit board) normally consists of two main part, namely analog radio front end and a digital signal processing back end (Nditiru, 2021) as shown in Figure 9 (b). In the typical SDR receiver, the analog radio front end is an RF tuner system that converts the received RF signal from antenna into an intermediate-frequency (IF) signal. Subsequently, IF signal is converted into digital signal using analog-to-digital converter (ADC). Then, digitized signal is channelled into the digital back end for processing (such as mixing, filtering and demodulation processes) using field-programmable gate array (FPGA) with on board digital signal processing (DSP) capabilities. On the other hand, if the SDR transceiver switches to transmitter mode (becomes an SDR transmitter), the digital modulation process (digital up-conversion) is first processed by the digital back-end. The digitally modulated IF signal from the digital back end is converted to an analog IF signal using a digital-to-analog converter (DAC). Then, the analog radio front end converts the analog IF signal into an RF signal, which is amplified by an amplifier, and then fed into the antenna for transmission.

Various Kinds of Low-Cost Software-Defined Radio (SDR)

Recently, there are a hundred kinds of SDRs on the market (Gannapathy *et al*., 2014). Here, only a few well-known and popular USB-based SDRs are listed in the Table 6, and their cost is less than 1000 USD. Each SDR has certain advantages and disadvantages. For instance, RTL-SDR has a large user community because of its small size (USB dongle), low price (~20 USD), simplicity, and extensive software support (GNU Radio and MATLAB Simulink). But, the weakness is narrow bandwidth and low dynamic range (low signal-to-noise ratio). If the amateur user would like to get a better reception signal, maybe the user can consider SDRPlay RSP1A (with ADC resolution of 14 bits). For professional and research implementations (while considering budget), Universal Software Radio Peripheral (USRP) B200 SDR is a good choice. One of the most popular SDRs at the moment is HackRF One, which is relatively low cost and able to cover the frequency range from 1 MHz to 6 GHz (online prices are between ~150 USD to ~350 USD). Besides, it is capable of using as a transmitter and receiver for various practical applications as well as can be become standalone SDR using extended touch screen LCD of PortaPack H2 firmware. In terms of overall performance and cost-effectiveness (price/performance ratio), HackRF One is still the best at the moment. Figure 10 shows a photo of the USRP B100 SDR (old version of USRP) and HackRF One SDR circuit.

In fact, apart from modulation and demodulation processing, SDR is a basic spectrum analyser (Sierra & Ramírez Arroyave, 2015; Majumber, 2018; Efrain Santos-Luna *et al*., 2019). If the SDR has a capable transmitter, Tx (built signal generator), such as USRP B200, BladeRF × 40, HackRF One, LimeSDR, and ADALM-PLUTO, then the SDR can also be used as a tracking signal or simple transceiver. Now, there is also a standalone spectrum analyzer built based on software-defined radio theory or technology, such as DEEPACE KC908 spectrum analyser, namely user can directly use the device function locked by manufacturer, user can also select editable mode to reconfigured the function of the device based on the needed of user.

Figure 9. (a) Traditional radio transceiver. (b) Software-defined radio transceiver
Terminology: **LO** *— Local Oscillator,* **IF** *— Intermediate-Frequency,* **ASIC** *— Application Specific Integrated Circuit,* **FPGA** *— Field Programmable Gate Array,* **DSP** *— Digital Signal Processor,* **GPP** *— General Purpose Processor*
(Rohde & Schwarz, 2004a).

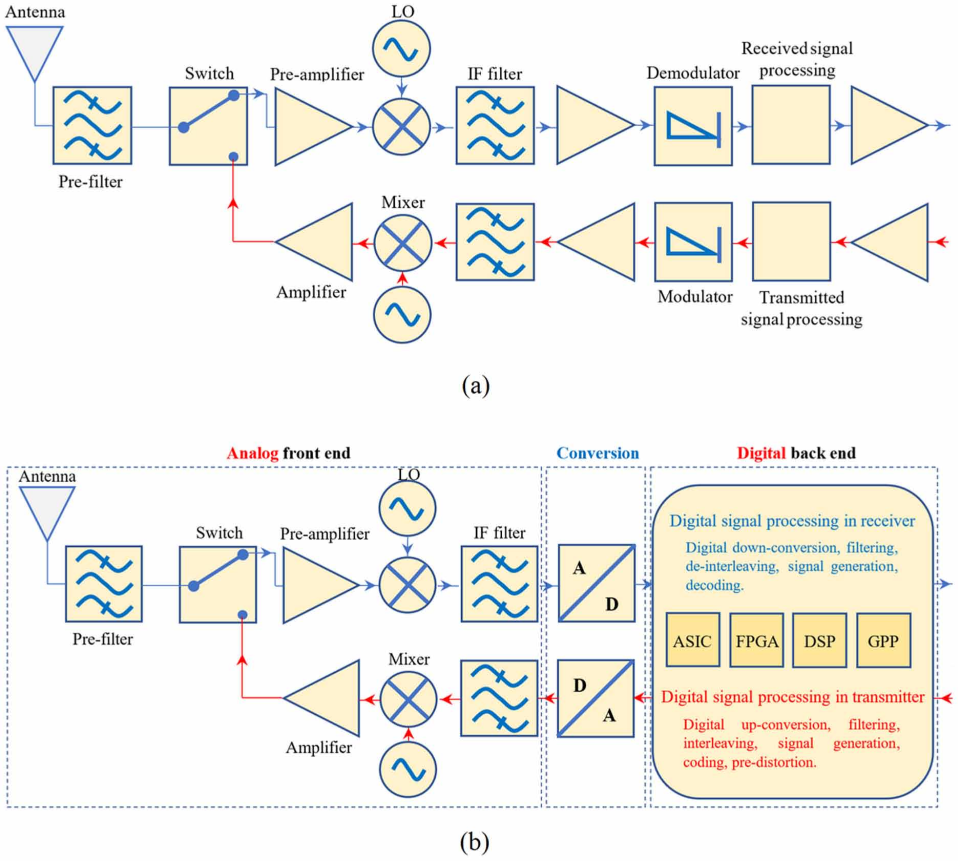

Antenna
LO
Received signal processing
Switch
Pre-amplifier
IF filter
Demodulator
Pre-filter
Mixer
Amplifier
Modulator
Transmitted signal processing
(a)
Analog front end
Conversion
Digital back end
Antenna
LO
Switch
Pre-amplifier
IF filter
Pre-filter
Digital signal processing in receiver
Digital down-conversion, filtering, de-interleaving, signal generation, decoding.
A
D
ASIC
FPGA
DSP
GPP
Mixer
D
A
Digital signal processing in transmitter
Digital up-conversion, filtering, interleaving, signal generation, coding, pre-distortion.
Amplifier
(b)

Figure 10. (a) USRP B100 software-defined radio (SDR) released in 2011 with a price of around 650 USD. (b) HackRF One SDR's circuit board.

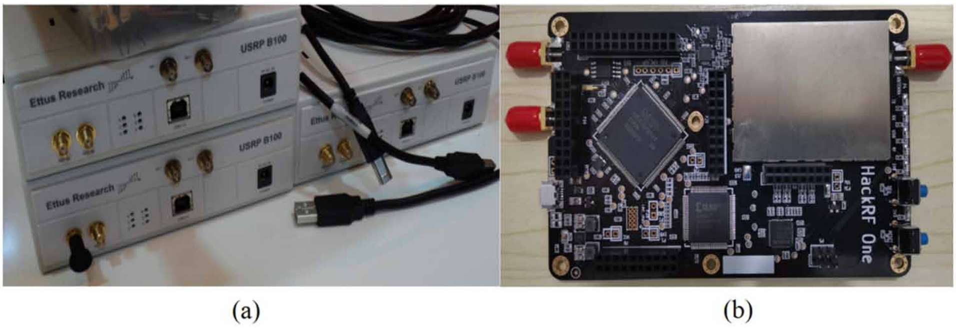


Table 6. Several low-cost USB-based SDRs (Price < 1000 USD)

Model	Frequency Range	Max. Bandwidth	ADC Resolution (Bits)	Processor	IC Chipset	Transmit Capable, Tx	Year	Price (USD)
FunCube Dongle Pro+	150 kHz – 260 MHz 410 MHz –2.05 GHz	192 kHz	16	-	MSi001 MSi2500	No	Late 2010	~210
RTL-SDR	500 kHz – 1.75 GHz	3.2 MHz	8	-	R820T2 RTL2832U	No	2012	~20
USRP B200	70 MHz – 6 GHz	56 MHz	12	Xilinx Spartan 6 XC6SLX75 FPGA	AD9364	Yes (Full Duplex)	2013	~675
BladeRF ×40	300 MHz – 3.8 GHz	40 MHz	12	Altera Cyclone 4 E FPGA	LMS6002M	Yes (Full Duplex)	2013	~420
HackRF One	1 MHz – 6 GHz	20 MHz	8	XC2C64A-7VQ100C CPLD	MAX5864 MAX2837 RFFC5072	Yes (Half Duplex)	2014	~300
AirSpy R1 (Latest AirSpy R2)	24 MHz – 1.75 GHz	10 MHz	12	-	R820T2 R860 Si5351C	No	Late 2014	~169
LimeSDR	100 kHz to 3.8 GHz	61.44 MHz	12	Altera Cyclone IV FPGA	LMS7002M	Yes (Full Duplex)	2016	~300
LimeSDR Mini	10 MHz to 3.5 GHz	30.72 MHz	12	Altera MAX 10 FPGA	LMS7002M	Yes (Full Duplex)	2017	~160

Continued on following page

Table 6. Continued

Model	Frequency Range	Max. Bandwidth	ADC Resolution (Bits)	Processor	IC Chipset	Transmit Capable, Tx	Year	Price (USD)
SDRPlay RSP1A	1 kHz – 2 GHz	10 MHz	14	-	MSi2500	No	2017	~100
ADALM-PLUTO (Pluto SDR)	325 MHz –3.8 GHz	20 MHz	12	Xilinx Zynq 7000	AD9363	Yes (Full Duplex)	Late 2017	~100 – 200

Processor Hardware Use in Software-Defined Radio (SDR)

Moreover, many types of compact universal microprocessors, such as the Arduino Mega 2560 and Raspberry Pi 4, are commercialized which can be implemented to replace PC in the parts of the data acquisition, mathematical calculation, and display (GUI controls). The integration between SDR module and portable microprocessor allows more small and creative projects can be developed in universities and industrial fields, such as some IoT-related projects. This situation will increase and diversify project activities within the university, and then narrow the gap between the university learning process and industrial product development. For instance, FlyDog SDR (derived from KiwiSDR) and RTL-SDR can be connected to the Raspberry Pi board used as the host processor (Sierra & Ramírez Arroyave, 2015). This kind of SDR is sometimes called "RaspberrySDR". In addition, RTL-SDR can also be integrated with Arduino and LCD to become a standalone SDR device.

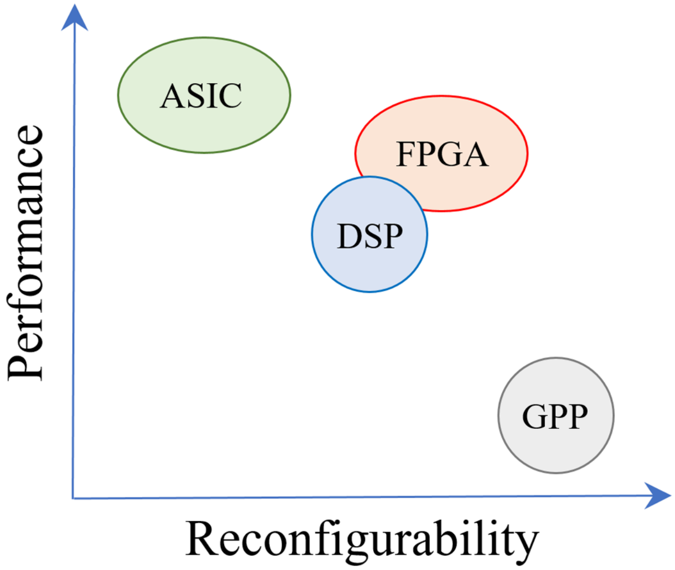
Normally, the single board module of SDR is equipped with FPGA and a GPS front-end chip, most of the digital operations are completed before the data is transferred to the computer (or Arduino or Raspberry Pi). Besides FPGA, there are another three kinds of processors and each has its own uses and operations in order to optimize their processing and computational power consumption, namely digital signal processor (DSP), general purpose processor (GPP), and application specific integrated circuit (ASIC) [See Figure 9 (b)]. The feature comparison between the four digital hardware is tabulated in Table 7 (Akeela, & Dezfouli, 2018).

Table 7. Features comparison between various types of digital processor hardware

No.	Feature		ASIC	FPGA	DSP	GPP
1	Performance		Very high	High	Medium high	Medium
2	Power consumption		Very low	Low	Medium low	Medium
3	Processing rate		Very high	High	Medium high	Medium
4	Flexibility		Very low	High	Very high	Very high
5	Reusability of programs		Medium	Medium	High	Very high
6	Execution		Single	Highly Parallel	Partially Parallel	Sequential
7	Cost	small quantities	Very high	Medium high	Medium	Medium
		large quantities	Low	Medium high	Medium	Medium
8	Brands and Model		SX-3000 ASIC	Airblue, Xilinx Zynq, Altera Cyclone	TMS320C6670, TMS320TCI100, ADSP-2191	x86/64, Advanced RISC Machine (ARM)

ASIC are not programmable and it is designed for particular application, after which they can be manufactured economically in large quantities. Hence, ASIC is normally applied in mobile phones. Recently, FPGA is widely implemented in SDR module. Although FPGA consume more power and occupy more area than ASIC, programmable features and highly parallel execution are the reasons why FPGA is widely used. In addition, the processing rate of FPGA is high compared to DSP and GPP. The main advantages of DSP and GPP are their flexibility and ease of configuration, as well as allowing better reuse of existing programs for other purposes. However, compared with GPP, DSP is a better choice for SDR deployment because DSP is particularly designed for digital signal processing. The performance versus re-configurability of the four processors hardware is simplify interpreted in Figure 11.

Figure 11. Comparison of FPGA, DSP, ASIC, and GPP for SDR implementation



Software for Software-Defined Radio (SDR)

In the development of SDR, software is also one of the important components that provide graphical interfaces, parameter/function settings, and mathematical calculation algorithm. Now, there is a lot of open-source and commercial SDR software available in the market, such as GNU Radio, MATLAB Simulink, LabView, SDRangel, Gqrx SDR, SDRSHARP (SDR#), CUDA, LegUP, Vivado HLS & SDSoC, Pothosware, HDSDR, and SDRConsole (V3). Further descriptions of SDR software and its applications can be found on the website:

https://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/
https://wiki.radioreference.com/index.php/SDR_Software_Applications

In general, each SDR module can be supported by more than one SDR software. For instance, ANTSDR E310 (derived from Pluto) is supported by GNU Radio, MATLAB Simulink, SDRangel, Gqrx SDR, SDR Sharp (SDR#), and Pothosware. On the other hand, FlyDog SDR (derived from KiwiSDR) can be connected and run smoothly with HDSDR, SDRConsole (V3), and SDRSHARP (SDR#).

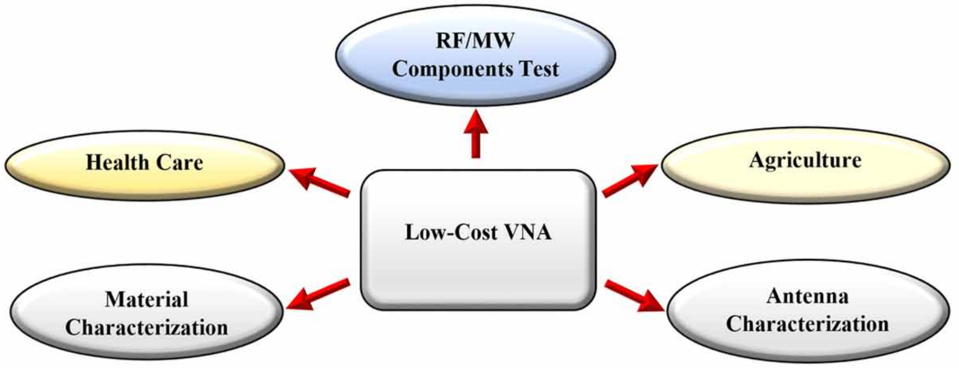
In the author's opinion, among most SDR software, GNU Radio is the most common and simple, because the software is open-source, programmable, can support most types of SDR modules and processor hardware (GPP, GPU, DSP, and FPGA), although GNU Radio's graphical interface is not the most beautiful and advanced compared to other. Similar to the MATLAB Simulink (Stewart *et al*., 2015), GNU Radio has built-in with various kinds of signal processing blocks, such as mathematical operations, different types of dialogue, signal generator, Fast Fourier transform (FFT), decoders, modulators, demodulators, and filters. Each block has inputs and outputs that can be associated with more varied types of data flows. From the connection between different basic blocks, a data flow diagram is formed, which defines the stages of signal processing of a given communication system. In addition, each block has a specific set of parameters that define its behavior. For instance, for the block representing the filter, there are some options that allow the user to select the desired filter characteristics, such as filter type, cutoff frequency, and transition band. In addition to these blocks provided by the software, other new blocks can be created by defining and adding new blocks through C++ or Python programming according to the needs of users.

AMATEUR DEVICES AND INSTRUMENTS APPLICATIONS

Low-Cost VNA Applications

In recent years, there have many researchers using low-cost VNA to perform RF/MW components test, antenna characterization, health care, agriculture, and material characterization shown in Figure 12. Depold *et al*. (2021) compared a low-cost vector network with Rohde & Schwarz (R&S) ZVB 8 measure of SAW 433 MHz band-pass filter and Mini-Circuits VLF-1700, Low pass filter DC to 1700 MHz. The measurement results indicated the SAW 433 MHz band-pass filter and Mini-Circuits VLF-1700 had almost similar matched passband and bandwidth between VNA two devices. However, the low-cost VNA shows a prominent ripple visible at the *S*-parameter of band-pass and low-pass filters over the frequency range compared to R&S ZVB 8. This is caused by the low-cost VNA using less than ideal calibration standards of short, open, load, and thru (SOLT).

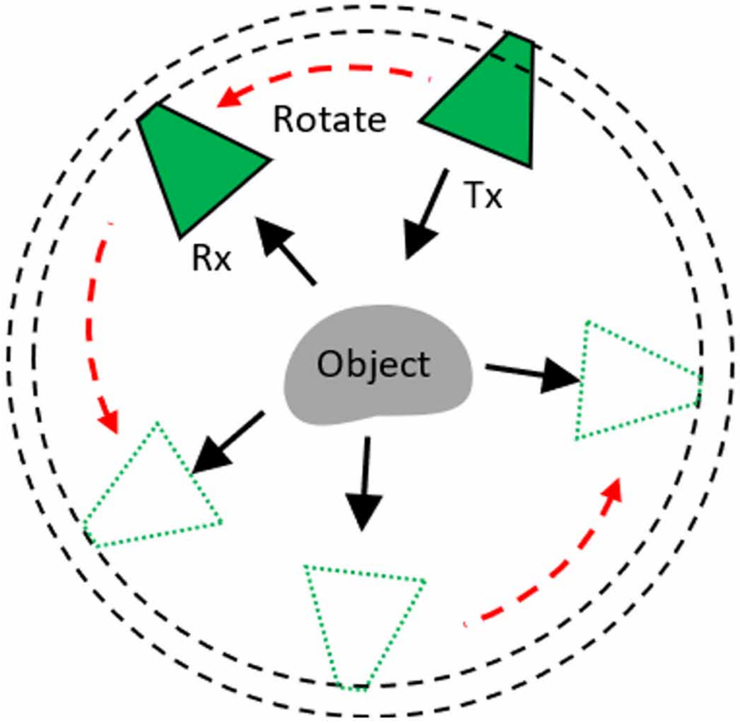
Figure 12. Low-cost VNA applications.



A study of developing a soil moisture measurement system with monopole probe, miniVNA Tiny, and Smartphone (Qiwei *et al*., 2019). The miniVNA Tiny is connected with USB to smartphone and SMA coaxial cable to a monopole antenna. The monopole probe is used as soil sensor and display data in smartphone via miniVNA Tiny android app. The study shows the antenna resistance resonances shift to the lower frequency as moisture content of soil increases over 1 MHz and 3 GHz frequency range. From the study, a calibration model of antenna probe resistance and soil moisture was developed based on measured data at 13 MHz. This linear model relates resistance and moisture content with the coefficient of determination value of 10.723 at 13 MHz.

Fikri *et al*. (2019) has developed a low-cost microwave tomography system based on Vivaldi antenna (1.5 GHz to 9 GHz), PocketVNA (500 kHz to 4 GHz), and Arduino Nano. The PocketVNA is used as data acquisition and Arduino Nano as a microcontroller to control the stepper motor of the Vivaldi antenna angular position. The circular path around the observed object is shown in Figure 13. The measurement in the study is to measure the magnitude and phase shift of the S-parameter (S_{11} and S_{21}) over 3 GHz to 3.78 GHz. One of the Vivaldi antennas is fixed at a position and another Vivaldi antenna is shifted every 5 degree of angle. In the study, the tested object used were octagonal iron metal, cylindrical metal, and nylon. The measured S-parameter is reconstructed to image processing based on the Born approximation algorithm which can illustrate the shape and cross-section of the tested object. The finding shows that the geometry of two different objects can be visualized.

Figure 13. The scanning process on measurement wave scattering data by test object.



Several researchers use low-cost VNA, such as PocketVNA to measure the dielectric properties of flaked canola seeds (Mohamed *et al.*, 2020). The PocketVNA is connected with a coaxial probe via coaxial cable and attached to the flake seeds. The results reported the value of dielectric properties increases when the flakes seeds are temperature is increasing (70 °C, 90 °C, and 100 °C). There have two different heating methods to heat up the flake seeds by using microwave and steam. The finding indicates that the flake seeds using microwave treatment has higher dielectric properties compared to steam treatment. This is due to MW disruption of the cell wall and release of the intercellular content. The research shows that PocketVNA can use to measure the *S*-parameters of flake seeds, perform calibration and use the *S*-parameter results to obtain dielectric properties.

Elsheakh *et al.* (2021) reported a rapid diagnostic device for the detection of the pandemic coronavirus (COVID-19) using a micro-immunosensor cavity resonator and pocket VNA. The system is a portable laboratory device for detecting the SARS-CoV-2 virus using a microwave cavity resonator (MCR) as a sensor at medical (ISM) 2.45 GHz. The measured results show air, buffer, -ve, and +ve biological samples affect the resonating frequency, magnitude, and phase of S_{11} (in unit dB) over 1.750

GHz to 2.5 GHz. The predictive accuracy of the system is 63.3% and 60.6% for the magnitude and phase of the reflection coefficient. The advantage of using the NanoVNA is portable, low cost, small size, light, rapid response, and customized software programs to operate automatically. The proposed technique provides real-time results with the merits of portability and eases to use.

Also, some researchers presented a method of quantifying blood glucose levels using a spiral microstrip antenna and PocketVNA with S_{11} parameters (Cordero *et al.*, 2017). The study analyzed two female subjects with a 20 kg difference in weight and body glucose level. Both subjects were tested using non-invasive and invasive blood glucose measurements. The spiral antenna is a non-invasive method that measured the skin with S_{11} parameters over 10 Hz to 1 GHz frequency spectrum. For blood glucose level using invasive method is monitored at 460 MHz to 480 MHz. It observed that the glucose level is directly proportional to the skin impedance in a certain frequency range. The research shows that with deeper analysis and machine learning in mathematical calculation. Able to provide a set of training data for analysis of skin impedance variation to predict the glucose level of the human body.

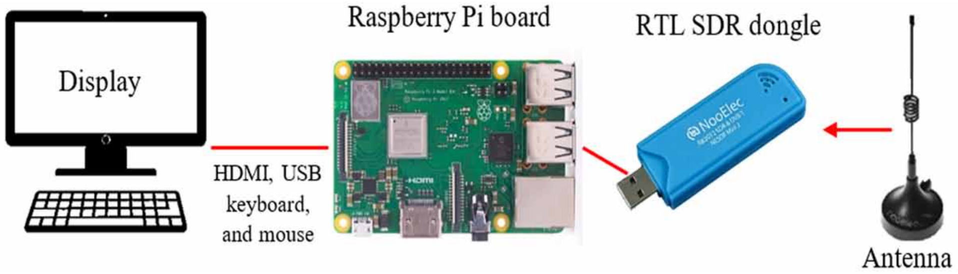
Amateur SDR Applications

The use of amateur SDR for 5G and IoT applications has gotten attention in recent years. Some examples of related works are described in this Sub-section. Gokceli *et al.* (2020) proposed an SDR prototype for clipped and fast-convolution filtered (OFDM) for 5G New Radio (NR) uplink. Marinho *et al.* (2020) used SDR to apply beamforming systems for 5G and radar applications. On the other hand, Ma et al. (2018) presented a multi-function radar for human body detection in human-centric IoT applications. For 5G multi-connectivity, SDR offers a cheaper approach than multiple base stations. SDRs can be used for the allocation of spectrum resources to multi-users. Due to the complex task, hardware accelerators are highly recommended to be used along with software (Chamola *et al.*, 2020).

The SDR signal processing can be performed using FPGA based hardware accelerator. Indoor positioning under the 5G new radio (NR) is one of the core technologies in the upcoming era of IoT and AI. The positioning based on 5G NR signals has drawn a lot of attention complexity of indoor environments is still the main challenge to achieve reliable indoor positioning. Chen *et al.* (2021) is proposed an SDR positioning system with 5G NR signals. Universal Software Radio Peripheral (USRP) is sampled and coarse synchronization is achieved to detect the synchronization signal block (SSB). The measurement setup is using SDR as a 5G NR receiver and an antenna as a 5G base station. The SDR system has been used for signal sampling and Recording based on USRP. The USRP can use for clock generation, digital-analog signal interfacing, power management, analog filtering, and up/down-conversion internal mixer. The SDR system with a specific configuration is able to adapt for sampling 5G NR SSB signals (Chen *et al*., 2021). The SDR act as a signal spectrum to receive the real-time transmission speed of 5G NR in an indoor field test at 2515-2675 MHz, China mobile frequency range. The test results show the time of arrival (ToA) accuracy for indoor positioning in 5G NR environment is about 0.5 meters.

In IoT application, Narayanan *et al*. (2020) has presented CharIoT with the distributed MIMO solution that mitigates collisions across low-power IoT radio technologies. Narayanan and her team used low-cost RTL-SDR as gateways and show simultaneous decoding of collision in indoor testbeds. The RTL-SDR gate was connected to a Raspberry Pi decodes collision of four popular IoT devices (LoRa, XBee, Z-Wave, and SIGFOX) in the 868 MHz ISM bands. Real-time energy detection spectrum sensing plays an important role in cognitive radio IoT (CR-IoT) nodes which allow cognitive users to identify the vacant frequency bands. Majumder (2018) proposed a CR-IoT using Raspberry Pi, RTL SDR, and GNU radio running on Ubuntu operating system. The Raspberry Pi act as a CR IoT terminal and the RTL SDR is used for energy detection spectrum sensing in CR enabled IoT terminal. The IoT terminal setup based on RTL-SDR and Raspberry Pi is shown in Figure 14.

Figure 14. IoT terminal setup based on RTL-SDR and Raspberry Pi.



CONCLUSION

In this chapter, the evolution of the development of several amateur RF/microwave instruments in twenty years has been described. Indeed, the development of SDR is strongly affected by the development of MMIC. For example, the first low-cost amateur VNAs, namely N2PK VNA and Ten-Tec 6000 were appeared due to the existence of stable and high-quality chipsets, such as AD9851/AD9854 direct digital synthesis (DDS) synthesizers (released in around 2000) and AD8302 gain and phase detector (released in 2001). Operating frequencies for amateur test instruments reach several GHz due to the existence of ADF4350 (in 2008) and HMC830L-P6GE (in 2011) wideband synthesizers.

Apart from the existence of MMIC, the construction of amateur instruments requires experts or technicians in the field of RF/microwave. As mentioned, recently most of our lives cannot avoid the use of wireless technology, the most notable is the use of smart phones and IoT devices. Hence, previously, most RF/microwave amateurs are built by retired specialists or technicians. However, nowadays, most of these devices are built by young enthusiasts who are interested in this field. Most small-scale amateur RF/Microwave test devices have been created through hobbies, self-learning, knowledge sharing, working experience, and crowd-funding. For instance, xaVNA and HackRF One were marketed through crowd-funding using the Kickstarter platform. While LimeSDR gets the development funding through the Crowd Supply platform. Donors are allowed to use the lowest price to get the final prototype test devices. Later, donors or users will provide valuable comments to improve the prototype based on use experience.

Most amateur RF/microwave devices are promoted and sold through online store platforms or personal blogs, so the price of devices are much cheaper than branders and professional RF/microwave devices. In addition, the quality and stability of the amateur devices are constantly improving. For example, analog PLL signal sources have been replaced by more accurate and stable DDS signal sources. Hardware-based devices have been replaced by digital software-based devices. In addition, the processor's ability to process digital signals is increasing, and the size of the processor chip is getting smaller and smaller. According to the development profile of MMIC (Analog Devices, 2021) and the recent amateur RF devices market, it is expected that a large number of low-cost amateur RF devices with operating frequencies up to millimeter wave (mmWave) will be released by 2024.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Akeela, R., & Dezfouli, B. (2018). Software-defined radios: Architecture, state-of-the-art, and challenges. *Computer Communications*, *128*, 106–125. doi:10.1016/j.comcom.2018.07.012

Armitage, S. (2006). Low-cost 2.4 GHz spectrum analyser. *Circuit Cellar*, *189*, 18–22.

Baier, T. C. (2007). A low budget vector network analyser for AF to UHF. *QEX*, 46–54.

Baier, T. C. (2009). A small, simple, USB-powered vector network analyser covering 1 kHz to 1.3 GHz. *QEX*, 32–36.

Castro. (2020). GPRS network prototype based on SDR and OpenBTS, as an IoT-lab Testbed. In *Seventh International Conference on Software Defined Systems (SDS)*. IEEE Publisher.

Chamola, V., Patra, S., Kumar, N., & Guizani, M. (2020). FPGA for 5G: Reconfigurable hardware for next generation communication. *IEEE Wireless Communications*, *27*(3), 140–147. doi:10.1109/MWC.001.1900359

Chen, L., Zhou, X., Chen, F., Yang, L.-L., & Chen, R. (2021). Carrier phase ranging for indoor positioning with 5G NR signals. *IEEE Internet of Things Journal.*

Cordero, C. J., Landicho, L. C. L., dela Cruz, J. C., & Garcia, R. G. (2017). Quantifying blood glucose level using S11 parameters. In *IEEE Region 10 Conference TENCON*. IEEE Publisher. doi:10.1109/TENCON.2017.8228091

Depold, A., Erhardt, S., Weigel, R., & Lurz, F. (2021). A 10kHz to 6GHz low-cost vector network analyzer. *Advances in Radio Science*, *19*, 17–22. doi:10.5194/ars-19-17-2021

Devices, A. (2021). *RF, microwave, and millimeter wave products: selection guide 2021*. RF, Microwave, and Millimeter Wave Products.

Elsheakh, D. M., Ahmed, M. I., Elashry, G. M., Moghannem, S. M., Elsadek, H. A., Elmazny, W. N., Alieldin, N. H., & Abdallah, E. A. (2021). Rapid detection of coronavirus (Covid-19) using microwave immunosensor cavity resonator. *Sensors (Basel)*, *21*(21), 7021. doi:10.339021217021 PMID:34770328

Fikri, D. N., Prajitno, P., & Wijaya, S. K. (2019). Development of microwave tomography system based on Arduino Nano and PocketVNA. In *2019 IEEE Conference on Antenna Measurements & Applications (CAMA)*. IEEE Publisher. 10.1109/CAMA47423.2019.8959618

Gannapathy, V. R., Tuani Ibrahim, A. F., Zakaria, Z., Othman, A. R., & Jalaudin, N. Q.Vigneswara Rao Gannapathy. (2014). A review on various types of software defined radios (SDRS) in radio communication. *International Journal of Research in Engineering and Technology*, *3*(12), 203–209. doi:10.15623/ijret.2014.0312026

Gavrila, C., Alexandru, M., Popescu, V., Sacchi, C., & Giusto, D. (2019). Satellite SDR gateway for M2M and IoT applications. In *IEEE Aerospace Conference*. IEEE Publisher. 10.1109/AERO.2019.8741705

Gokceli, S., Campo, P. P., Levanen, T., Yli-Kaakinen, J., Turunen, M., Allen, M., Riihonen, T., Palin, A., Renfors, M., & Valkama, M. (2020). SDR prototype for clipped and fast-convolution filtered OFDM for 5G New Radio uplink. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 89946–89963. doi:10.1109/ACCESS.2020.2993871

Henze, A., Tempone, N., Monasterios, G., & Silva, H. (2014). Incomplete 2-port vector network analyzer calibration methods. In *IEEE Biennial Congress of Argentina (ARGENCON)*. IEEE Publisher. 10.1109/ARGENCON.2014.6868593

International Telecommunication Union. (2009). *Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)*. Report ITU-R SM.2152.

Krok, M., & Gwarek, W. (2006). A low-cost PC controlled system for measurement of vector reflection coefficient in ISM band. In *International Conference on Microwaves, Radar & Wireless Communications*. IEEE Publisher. 10.1109/MIKON.2006.4345099

Ma, Y., Zeng, Y., & Sun, S. (2018). A software defined radio based multi-function radar for IoT applications. In *24th Asia-Pacific Conference on Communications (APCC)*. IEEE Publisher. 10.1109/APCC.2018.8633541

Majumber, S. (2018). Energy detection spectrum sensing on RTL-SDR based IoT platform. In *Conference on Information and Communication Technology*. IEEE Publisher.

Marinho, D., Arruela, R., Varum, T., & Matos, J. N. (2020). Software-defined radio beamforming system for 5G/radar applications. *Applied Sciences (Basel, Switzerland)*, *10*(20), 7187. doi:10.3390/app10207187

McDermott, T. & Ireland, K. (2004). A low-cost 100 MHz vector network analyzer with USB interface. *QEX*, 3–14.

Mitola, J. (1993). Software radios: Survey, critical evaluation and future directions. *IEEE Aerospace and Electronic Systems Magazine*, *8*(4), 25–36. doi:10.1109/62.210638

Mohamed, M. A., Knoerzer, K., Mansour, M. P., Trujillo, F. J., Juliano, P., & Shrestha, P. (2020). Improved canola oil expeller extraction using a pilot-scale continuous flow microwave system for pre-treatment of seeds and flaked seeds. *Journal of Food Engineering*, *284*, 110053. doi:10.1016/j.jfoodeng.2020.110053

Narayanan, R., Kumar, S., & Murthy, S. R. (2020). Cross technology distributed MIMO for low power IoT. *IEEE Transactions on Mobile Computing*.

Nditiru, S. (2021). SDRs as a reference and common clock source for GNSS timing apps. *Microwaves & RF*, 20–24.

Park, Y. T., Kuk, S. H., Kang, I. H., & Kim, H. G. (2017). Overcoming IoT language barriers using smartphone SDRs. *IEEE Transactions on Mobile Computing*, *16*(3), 816–828. doi:10.1109/TMC.2016.2570749

Qiwei, Z., Faiz Zainuddin, M., Fahad Ahmad, A., Obays, S. J., & Abbas, Z., Qiwei, Z., Zainuddin, M. F., & Ahmad, A. F. (2019). Development of an Affordable Soil Moisture Sensor System with Mini-VNA Tiny and Smartphone. *Pertanika Journal of Science & Technology*, *27*(3), 1121–1129.

Reite, B. (2019). PocketVNA review. *Radio Guide*, *27*(5), 14.

Rohde & Schwarz. (2004a). Software defined radios – overview and hardware. *New from Rohde & Schwarz*, *182*, 58–61.

Rohde & Schwarz. (2004b). Software defined radios – software aspects and the future. *New from Rohde & Schwarz*, *183*, 52–55.

Rytting, D. (2001). VNA error models and calibration methods. In *Proc. ARFTG/NIST Short Course on RF Measurements for a Wireless World*. IEEE Publisher.

Salas, P. (2011). Array Solutions VNA 2180 vector network analyser. *QST*, 57–59.

Salas, P. (2020). NanoVNA vector network analyser. *QST*, 39–43.

Santos-Luna, E. (2019). A spectrum analyser based on a low-cost hardware-software integration. In *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE Publisher.

Sierra, E. G., & Ramírez Arroyave, G. A. (2015). Low cost SDR spectrum analyzer and analog radio receiver using GNU radio, Raspberry Pi2 and SDR-RTL dongle. In *7th IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE Publisher. 10.1109/LATINCOM.2015.7430125

Steber, G. R. (2020). An ultra low cost vector network analyser. *QEX*, 3–9.

Stewart, R. W., Crockett, L., Atkinson, D., Barlee, K., Crawford, D., Chalmers, I., Mclernon, M., & Sozer, E. (2015). A low-cost desktop software defined radio design environment using MATLAB, Simulink, and the RTL-SDR. *IEEE Communications Magazine*, *53*(9), 64–71. doi:10.1109/MCOM.2015.7263347

You, K. Y. (2017). Materials characterization using microwave waveguide system. In S. Goudos (Ed.), *Microwave systems and applications* (pp. 341–358). IntechOpen. doi:10.5772/66230

You, K. Y., Derek Ng, Y. S., Lee, C. Y., Abbas, Z., Cheng, E. M., Lee, Y. S., & Lee, K. Y. (2017). Low-cost vector network analyser for communication devices testing – brief review. *International Journal of Advances in Microwave Technology*, *2*(1), 93–97.

ADDITIONAL READING

Aryanfar, F., Cepni, A. G., & Buris, N. E. (2008). Design and implementation of a low cost portable material analyser. *IEEE Antennas and Propagation Society International Symposium*. IEEE Publisher. 10.1109/APS.2008.4619796

Ben-Aboud, Y., Ghogho, M., Pollin, S., & Kobbane, A. (2021). Electro-Smog monitoring using low-cost software-defined radio dongles. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 107149–107158. doi:10.1109/ACCESS.2021.3100773

Depold, A., Erhardt, S., Weigel, R., & Lurz, F. (2021). A 10 kHz to 6 GHz low-cost vector network analyser. *Advances in Radio Science*, *19*, 17–22. doi:10.5194/ars-19-17-2021

Feng, W. K., Friedt, J. M., Goavec-Meron, G., & Meyer, F. (2021). Software-defined radio implemented GPS spoofing and its computationally efficient detection and suppression. *IEEE Aerospace and Electronic Systems Magazine*, *36*(3), 36–52. doi:10.1109/MAES.2020.3040491

Feng, W. K., Friedt, J. M., & Wan, P. C. (2021). SDR-implemented ground-based interferometric radar for displacement measurement. *IEEE Transactions on Instrumentation and Measurement*, *70*, 70. doi:10.1109/TIM.2021.3069805

Fujii, Y., Iye, T., Tsuda, K., & Tanibayashi, A. (2021). 28 GHz cooperative digital beamforming for 5G advanced system on an SDR platform. In *IEEE Radio and Wireless Symposium (RWS)*. IEEE Publisher. 10.1109/RWS50353.2021.9360368

Hindle, P. (2020). Very low-cost RF test equipment for the DIY engineer or student (<$1,000). *Microwave Journal*.

Malik, H., & Burki, J. (2020). Concept paper IEEE radar challenge 2020 Radar-A-Thon. In *2020 IEEE International RADAR Conference*. IEEE Publisher.

Panchenko, S., & Cheranev, A. (2021). Interception wideband FM signals with RTL-SDR. In *Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*. IEEE Publisher. 10.1109/USBEREIT51232.2021.9455110

Robert, M., Sun, Y., Goodwin, T., Turner, H., Reed, J. H., & White, J. (2015). Software frameworks for SDR. *Proceedings of the IEEE*, *103*(3), 452–475. doi:10.1109/JPROC.2015.2391176

Schmidth, E., Ruble, Z., Akopian, D., & Pack, D. J. (2019). Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study. *IEEE Transactions on Instrumentation and Measurement*, *68*(8), 2768–2784. doi:10.1109/TIM.2018.2869261

Will, K., Meyer, T., & Omar, A. (2008). Low-cost high-resolution handheld VNA using RF interferometry. *IEEE MTT-S International Microwave Symposium Digest*. IEEE Publisher. 10.1109/MWSYM.2008.4633181

Wright, D. P., & Ball, E. A. (2020). Highly portable, low-cost SDR instrument for RF propagation studies. *IEEE Transactions on Instrumentation and Measurement*, *69*(8), 5446–5457. doi:10.1109/TIM.2019.2959422

You, K. Y. (2016). *RF coaxial slot radiators: Modeling, measurements, and applications*. Artech House.

You, K. Y. (2018). Introductory chapter: RF/microwave applications. In K. Y. You (Ed.), *Emerging microwave technologies in industrial, agricultural, medical and food processing* (pp. 1–7). IntechOpen. doi:10.5772/intechopen.73574

Young, A. R., & Bostian, C. W. (2013). Simple and low-cost platforms for cognitive radio experiments. *IEEE Microwave Magazine*, *14*(1), 146–157. doi:10.1109/MMM.2012.2226543

Zitouni, R., & George, L. (2016). Output power analysis of a software defined radio device. In *IEEE Radio and Antenna Days of the Indian Ocean (RADIO)*. IEEE Publisher. doi:10.1109/RADIO.2016.7771996

KEY TERMS AND DEFINITIONS

Application-Specific Integrated Circuit (ASIC): An integrated circuit (IC) chip customized for a specific use or application.

Digital Signal Processor (DSP): A microprocessor chip is used for digital signal processing.

Field-Programmable Gate Array (FPGA): A programmable logic integrated circuit (IC) which can be re-configured by the user or designer after manufacturing.

Fifth Generation Wireless Technology (5G): Digital cellular mobile communication networks that began wide deployment in 2019.

Fourth Industrial Revolution (Industry 4.0): A major shift in industrial development tends to enable automation and data exchange in manufacturing technologies and processes, including cyber physical systems (CPS), industrial Internet of things (IIOT), cloud computing, cognitive computing, and artificial intelligence.

General Purpose Processor (GPP): A processor chip for general purpose computers such as PCs or workstations.

Industrial Internet of Things (IIoT): An Internet of Things (IoT) for industrial applications.

Internet of Everything (IoE): A concept that extends the Internet of Things (IoT).

Internet of Things (IoT): A system of interrelated computing devices, mechanical, and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Microwave (MW): A form of electromagnetic radiation with wavelengths ranging from 1 m to 1 mm, which is corresponding to operating frequencies ranging from 300 MHz to 300 GHz.

Microwave-Integrated Circuit (MIC): An integrated circuit (IC) chip that operates at microwave frequencies.

Millimeter Wave (mmWave): A form of electromagnetic radiation with wavelengths ranging from 10 mm to 1 mm, which is corresponding to operating frequencies ranging from 30 GHz to 300 GHz (within UHF and EHF bands of microwave).

Radio Frequency (RF): A part of the electromagnetic spectrum from about 3 kHz to 300 MHz, which is corresponding to wavelengths ranging from 100 km to 1 m.

Scattering Parameters (S-Parameters): A parameter that describes the electrical behaviour of linear electrical networks when subjected to various steady-state stimuli by electrical signals.

Sixth Generation Wireless Technology (6G): A successor to 5G cellular technology, in which it is expected to be extended the operating frequency up to 3 THz (or above) with data rates of 0.1–1 Tbps, spectrum efficiency of 3–60 bps/Hz, 100 GHz channel bandwidth, and 1000 km/h mobility.

Software-Defined Radio (SDR): A radio communication system in which some components traditionally implemented in hardware, such as mixers, filters, and amplifiers, are instead implemented in software on a personal computer or embedded system.

Spectrum Analyser (SA): A test instrument that measures the power amplitude of an input signal in the frequency domain (sweep over a certain frequency range) to analyse the frequency spectrum, dominant frequency, power level/strength, distortion, harmonics, and bandwidth of the electrical signals.

Vector Network Analyser (VNA): A vector test instrument that measures the response of a network as S-parameters so that its performance can be characterized.

Chapter 9
Tunable Attenuator Based on Hybrid Metal-Graphene Structure on Spoof Surface Plasmon Polaritons Waveguide

Aymen Hlali
University of Carthage, Tunisia

Hassen Zairi
University of Carthage, Tunisia

ABSTRACT

A novel type of tunable attenuator on spoof surface plasmon polaritons (SSPP) waveguide based on hybrid metal-graphene structure for terahertz applications is proposed in this chapter. Two structures are analyzed and designed, where the first is composed of a graphene sheet at only one cell of the SSPP waveguide and the second at all cells. By varying the graphene chemical potential via a biased voltage, the surface conductivity of graphene can be adjusted. Therefore, the attenuation can also be adjusted. Moreover, an equivalent circuit model is proposed to facilitate the designs of the proposed attenuator and offer a general understanding of the attenuation mechanism. Numerical simulation results with the CST simulator and WCIP method have a good agreement with the theoretical results. The simulated results show that the attenuator can obtain an adjustment range from 6.02 to 14.32 dB for the first structure and from 1.58 to 30.93 dB for the second, as the chemical potential rises from 0 to 0.5 eV.

DOI: 10.4018/978-1-6684-3855-8.ch009

INTRODUCTION

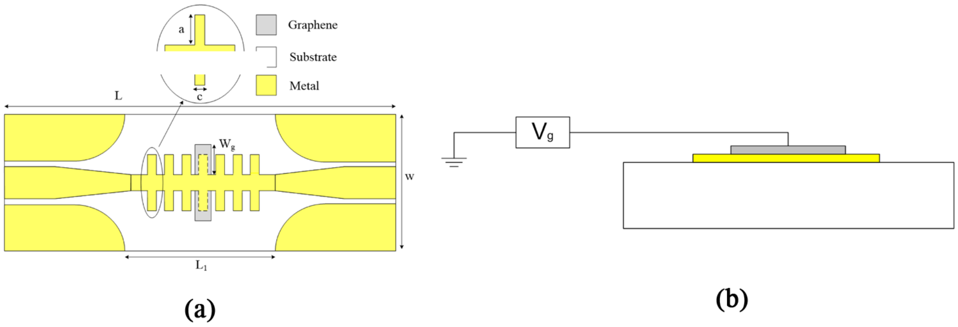
Spoof Surface Plasmon Polaritons (SSPPs) have attracted increasing attention due to their exceptional capability of guiding electromagnetic waves, flexibility enhancement, and mutual coupling reduction (Chen et al., 2018; Tang et al., 2019). Several groups developed many microwave components and devices based on the SSPP concept, such as antennas, waveguides, sensors, filters, splitters, and couplers (Kianinejad et al., 2015; Kianinejad et al., 2018; Zhang et al., 2017). A reconfigurable SSPP waveguide attenuator is a fundamental component for microwave applications. As a two-dimensional material with several interesting characteristics, Graphene has been widely used in the manufacture of microwave and terahertz components. In fact, it is considered an electronically tunable component thanks to one of its key characteristics, which is its ability to change its conductivity. A number of graphene-based tunable attenuators have been proposed in (Zhang et al., 2019a; Zhang et al., 2019b; Zhang et al., 2018; Zhang et al., 2019).

Similarly, the tunable substrate integrated waveguide attenuator using Graphene mentioned in (Zhang et al., 2018), were obtained by depositing two graphene sandwich structures inside a Substrate Integrated Waveguide (SIW). The attenuator in reference (Zhang et al., 2019a) consists of a microstrip line and two graphene sandwich structures. In fact, these graphene sandwich structures are placed on the substrate of the microstrip line, close to the signal strip over the propagation direction. Reference (Zhang et al., 2019) has proposed and realized a flexible and tunable attenuator construct on graphene-based spoof surface plasmon polaritons waveguide. This attenuator is built by making a graphene sandwich structure on an SSPP waveguide. All of these structures operate in the bands 7-14, 10-40, and 6-9 GHz, respectively. However, though it has not been developed, a Terahertz tunable attenuator is a fundamental device for an RF system. To the authors' knowledge, until the time of writing this Chapter, no work has been developed on a tunable attenuator based on SSPP designs in the THz band. In this work, a novel type of tunable attenuator based on a hybrid metal-graphene structure on spoof surface plasmon polaritons waveguide is proposed. This type of attenuator is developed to operate in the terahertz band. The theoretical analysis of the graphene-based attenuator demonstrated that the attenuation could be adjusted by adding graphene cells over the SSPP waveguide and by varying the graphene chemical potential. In order to validate the accuracy and efficiency of our study, the extracted analytic results are comprehensively compared with the simulated results with the Wave Concept Iterative Process (WCIP) method and CST simulator. This paper is organized as follows. In section II, the theoretical analysis of the structures and some theoretical aspects of the Graphene and WCIP method are presented. Subsequently, numerical results are introduced in section III to demonstrate the effect of graphene chemical potential variation and the number of cells on attenuation. Eventually, conclusions are provided at the end of this paper.

THEORY AND FORMULATION

Figure 1 illustrates a schematic configuration of the proposed SSPP waveguide, composed of a metal strip with periodic square cells. The golden area represents the metal, the gray area stands for Graphene, and the white area describes the dielectric substrate. Here, we choose Arlon as the substrate with a thickness of 2.8 µm and relative permittivity of 3.

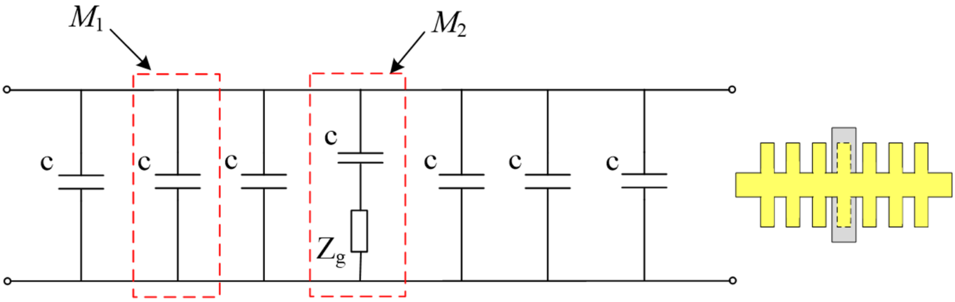
Figure 1. Schematic configuration of the proposed attenuator: (a) Top view and (b) side view.



As shown in Fig. 1, the graphene layer is placed on the SSPP waveguide. The parameters of the proposed attenuator are designed as: L = 66, L1 = 26.2, W = 23.4, Wg = 2.7, h = 2.8, a = 2.7, c = 1, all in micrometers.

An equivalent circuit model is proposed to offer a general understanding and facilitate the designs and optimizations with desired performance. The equivalent circuit of the attenuator with a graphene sheet at only one cell of the SSPP waveguide is shown in Fig. 2.

Figure 2. Equivalent circuit of the attenuator with a graphene sheet at only one cell of the SSPP waveguide.



As seen in Fig. 2, each unit cell M_1 consists of a length l, and it is composed of three matrices. Equation (1) represents this model, where Z_0 and β are the characteristic impedance and the phase constant (Pozar, 2011)

$$M_1 = \begin{bmatrix} \cos\beta l & jZ_0 \sin\beta l \\ j\dfrac{1}{Z_0}\sin\beta l & \cos\beta l \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ \dfrac{j}{Z_0 \tan\beta\alpha} & 1 \end{bmatrix} \times \begin{bmatrix} \cos\beta l & jZ_0 \sin\beta l \\ j\dfrac{1}{Z_0}\sin\beta l & \cos\beta l \end{bmatrix} \tag{1}$$

To include the Graphene in the equivalent circuit model, we add loading impedance to the shunt lines. M_2 is also composed of three matrices, explained by Equation (2)

$$M_2 = \begin{bmatrix} \cos\beta l & jZ_0 \sin\beta l \\ j\dfrac{1}{Z_0}\sin\beta l & \cos\beta l \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ \dfrac{j}{Z_{ing}} & 1 \end{bmatrix} \times \begin{bmatrix} \cos\beta l & jZ_0 \sin\beta l \\ j\dfrac{1}{Z_0}\sin\beta l & \cos\beta l \end{bmatrix} \tag{2}$$

where Z_{ing} is the input impedance toward the graphene cell that can be calculated by

$$Z_{ing} = Y_0 \frac{Z_0 + jZ_g \tan\beta W_g}{Z_g + jZ_0 \tan\beta W_g} \tag{3}$$

where $Z_g = 1/\sigma_g$ is the surface impedance of Graphene and $Y_0 = 1/Z_0$ is the line characteristic admittance.

In the range of frequency below 8 THz, the intraband conductivity dominates the overall conductivity, and the interband conductivity has no impact on the total conductivity within this band (Hlali et al., 2019a). The intraband term can be evaluated as

$$\sigma_g = \sigma_{intra} = -j\frac{e^2 K_B T}{\pi\hbar^2\left(\omega - j2\Gamma\right)}\left[\frac{\mu_c}{K_B T} + 2\ln\left(e^{-\frac{\mu_c}{K_B T}} + 1\right)\right] \tag{4}$$

Equation 5 represents the matrix of the complete structure

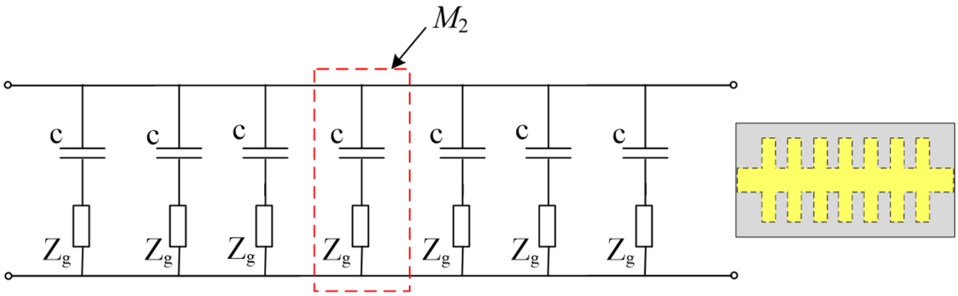
$$M_{tot} = M_1 \times M_1 \times M_1 \times M_2 \times M_1 \times M_1 \times M_1 \tag{5}$$

The attenuator is a reciprocal ($S_{21} = S_{12}$) and symmetrical network ($S_{11} = S_{22}$). Thus, its S_{21} can be obtained by the matrix conversion from the ABCD matrix (Pozar, 2011) as follows

$$S_{21} = \frac{2}{A + \frac{B}{Z_0} + CZ_0 + D} \tag{6}$$

Fig. 3 depicts the equivalent circuit of the attenuator with a graphene sheet at all cells of the SSPP waveguide.

Figure 3. Equivalent circuit of the attenuator with a graphene sheet at all cells of the SSPP waveguide.



The ABCD parameters of the overall structure matrix can be computed using the network analysis

$$M_{tot} = M_2 \times M_2 \times M_2 \times M_2 \times M_2 \times M_2 \times M_2 \tag{7}$$

Solving (7), the attenuation constant *P* of the equivalent circuits presented in Figs. 2 and 3 can be calculated by the scattering parameters, which is defined as $P=-20 \log |S_{21}|$ (Pozar, 2011).

The WCIP method has been described in various articles (Hlali et al., 2018; Hlali et al., 2019a; Hlali et al., 2019b). Graphene is implemented in the WCIP method as a boundary condition via the electric field and the current density using the surface conductivity. It has been fully explained in these articles (Hlali et al., 2018; Hlali et al., 2019a). The scattering matrix of Graphene is

$$\hat{S}_g = \begin{pmatrix} S_{11}^G & S_{12}^G \\ S_{21}^G & S_{22}^G \end{pmatrix}$$

where S_{ij} are defined by

$$S_{11}^G = \frac{Z_{02} - Z_{01} - \sigma Z_{02} Z_{01}}{Z_{02} + Z_{01} + \sigma Z_{02} Z_{01}}$$

$$S_{12}^G = \frac{2 Z_{02} \sqrt{Z_{01}}}{\sqrt{Z_{02} \left(Z_{02} + Z_{01} + \sigma Z_{02} Z_{01} \right)}}$$

$$S_{21}^G = \frac{2 Z_{01} \sqrt{Z_{02}}}{\sqrt{Z_{02} \left(Z_{02} + Z_{01} + \sigma Z_{02} Z_{01} \right)}}$$

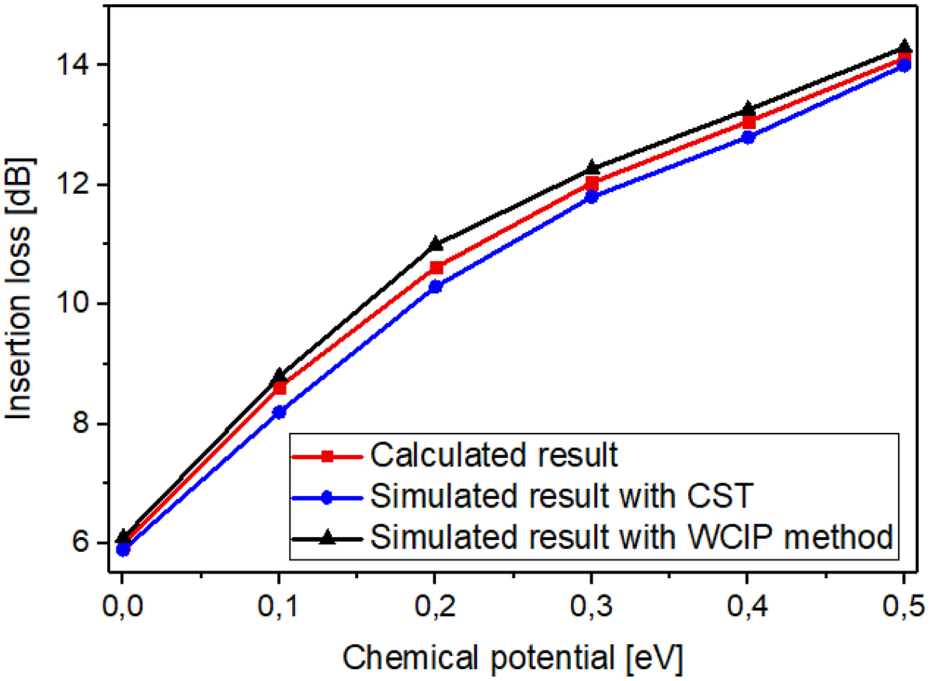
$$S_{22}^G = -\frac{Z_{02} - Z_{01} + \sigma Z_{02} Z_{01}}{Z_{02} + Z_{01} + \sigma Z_{02} Z_{01}}$$

When a layer of metal is placed below a layer of Graphene, the scattering matrix of this hybrid form considers the boundary conditions of Graphene in medium 1 and the boundary conditions of metal in medium 2.

NUMERICAL RESULTS AND DISCUSSION

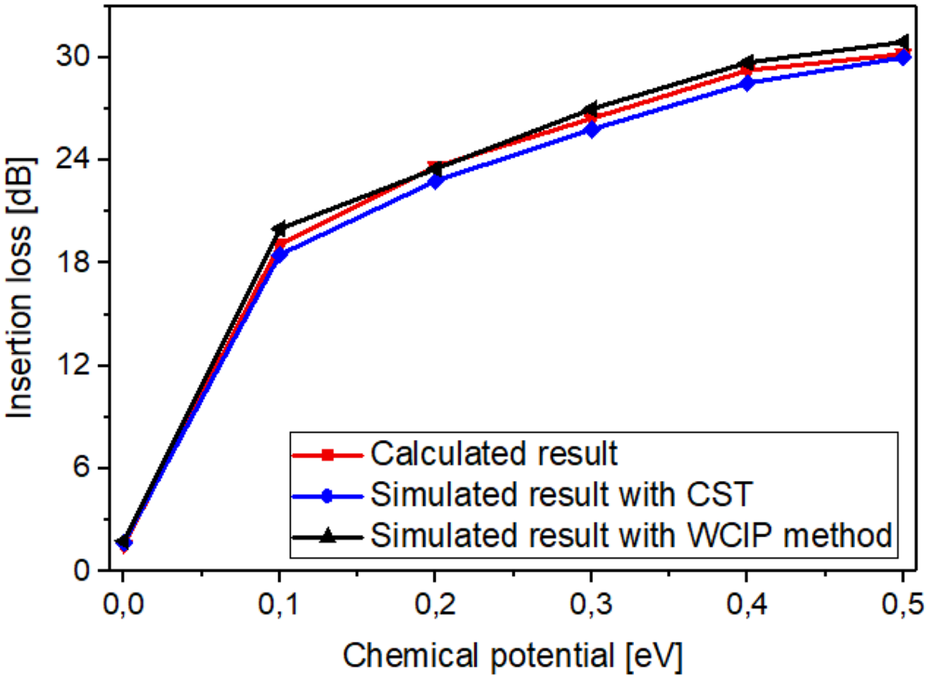
To validate the theoretical analysis presented above, the WCIP method and CST Microwave Studio are utilized to perform the simulation. Fig. 4 shows the calculated and simulated results of the attenuator at 2 THz with a graphene sheet at only one cell of the SSPP waveguide versus different chemical potential values.

Figure 4. Insertion loss of the attenuator with a graphene sheet at only one cell of the SSPP waveguide versus different chemical potential values.



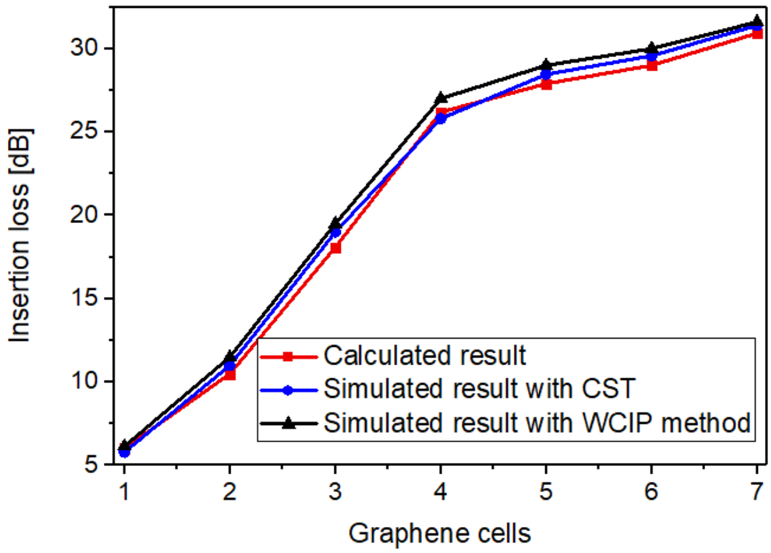
As shown in Fig. 4, there is a good agreement between the calculated results and the simulated results obtained by the WCIP method and the CST simulator. We also note that graphene conductivity has an important effect on attenuation. As the chemical potential of Graphene μc increases from 0 to 0.5 eV, the insertion loss increases from 6.02 to 14.32 dB. We notice that the chemical potential depends on the carrier density, which a bias voltage can control. The variation of the attenuation can be explained based on physical interpretation. When the chemical potential of graphene μc approaches zero, the impedance of Graphene is high. Then, the current density is almost zero. In this case, the insertion loss of the attenuator is at its lowest level. As the chemical potential μc increases, the surface impedance progressively decreases. As a result, the current density increases. Thus, the insertion loss gradually increases.

Figure 5. Insertion loss of the attenuator with a graphene sheet at all cells of the SSPP waveguide versus different values of chemical potential.



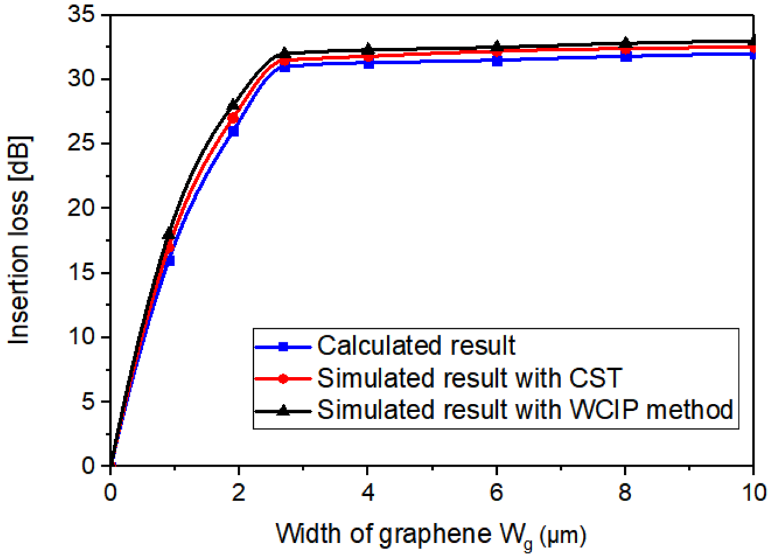
It can be clearly demonstrated that this attenuator can achieve an attenuation range from 1.58 to 30.93 dB while the chemical potential of Graphene is changing from 0 to 0.5 eV. In order to demonstrate the effect of the graphene cells number on attenuation, Fig. 6 shows the calculated and simulated insertion loss as a function of the number of graphene cells, where the graphene chemical potential is 0.5 eV.

Figure 6. Insertion loss of the attenuator versus the number of graphene cells.



We can note that the insertion loss increases when the number of graphene cells increases; thus, the regulation band rises. In addition, the effect of the width of the graphene sheet at 2 THz is studied in Figure 7.

Figure 7. Insertion loss of the attenuator with a graphene sheet at all cells of the SSPP waveguide versus width of the graphene sheet.



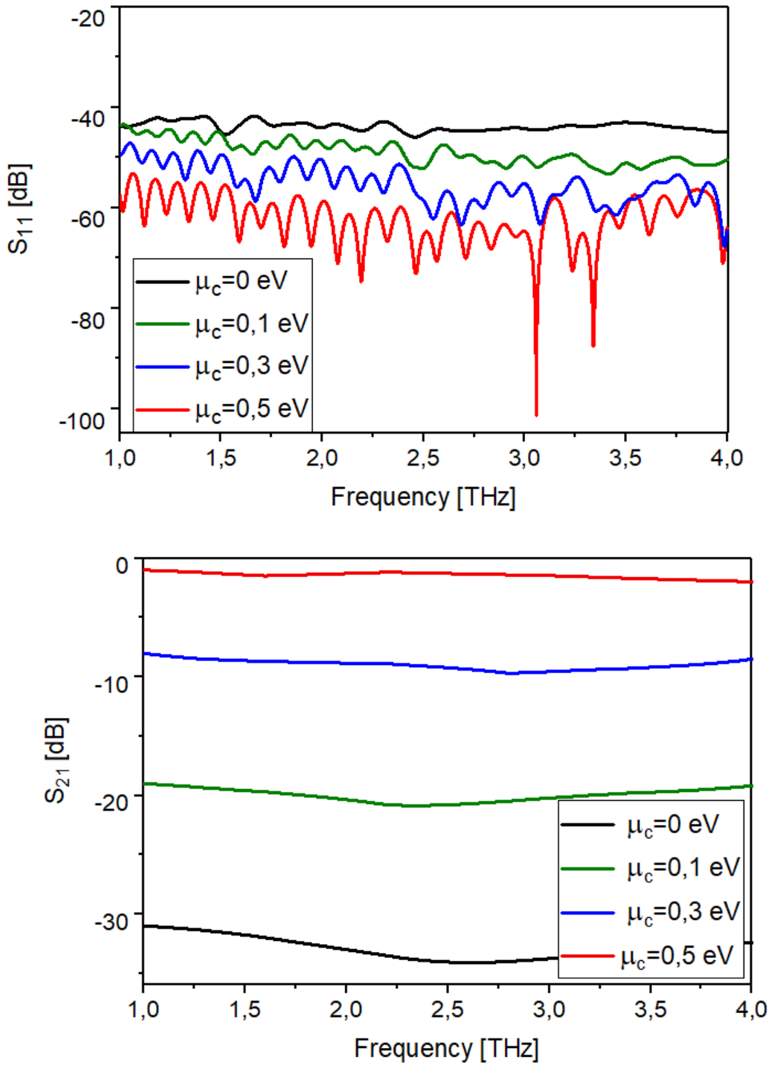
The result shows that by increasing the width of graphene sheet Wg, the insertion loss increases as the width of Graphene Wg increases from 0 μm to Wg' a. After this value, the insertion loss remains almost unchanged. Table 1 presents the comparison results of the performance comparison of the proposed attenuator with a graphene sheet at only one cell and at all cells of the spoof surface plasmon polaritons waveguide, and without Graphene.

Table 1. Performance characteristics of the three configurations.

Structure	$\|S_{21}\|$ Range	$\|S_{11}\|$	Frequency Band
	(dB)	(dB)	(THz)
Without graphene	non-tunable	<-15	2 – 4
Graphene at one cell	6.02 - 14.32	<-40	2 – 4
Graphene at all cells	1.58 - 30.93	<-50	2 – 4

According to the results obtained above, it can be seen that the proposed attenuator with a graphene sheet at all cells gives a wider tunable attenuation range which increases from 6.02-14.32 dB to 1.58-30.93 dB, and a low return loss when compared with the attenuator with a graphene sheet at one cell. Further, Fig. 8 shows the variation of the reflection and transmission coefficients of the attenuator with a graphene sheet at all cells operating from 1 to 4 THz for different chemical potentials.

Figure 8. Simulated results for different chemical potentials: (a) Reflection coefficient and (b) transmission coefficient.



As shown in Fig. 8 (b), the magnitude of transmission coefficient can be tuned from 1.58 to 30.9 dB with a reflection below 40 dB, when the chemical potential μc increases from 0 to 0.5 eV. The return loss characteristics decrease by increasing the chemical potential.

CONCLUSION

A novel type of tunable attenuator on spoof surface plasmon polaritons waveguide based on hybrid metal-graphene structure for terahertz applications is discussed in this paper. We produce this attenuator by depositing a graphene sheet at only one cell of the SSPP waveguide or all cells. Equivalent circuit models for the two structures are provided to analyze the performance of this attenuator. Based in these models, the influences of the graphene chemical potential, the number of graphene cells, and the width of the graphene sheet on the insertion loss of the attenuator are analyzed by comparing the calculated result with the simulated results obtained by the CST simulator and WCIP method. In accordance with the analysis, the attenuation can be adjusted by varying the graphene chemical potential. The attenuator with a graphene sheet at all cells exhibits good performance than the other attenuator, where it gives a wider tunable attenuation range which increases from 6.02-14.32 dB to 1.58-30.93 dB and low return loss.

REFERENCES

Chen, H., Lu, W. B., Lui, Z. G., Zhang, J., & Huang, B. H. (2018). Efficient Manipulation of Spoof Surface Plasmon Polaritons Based on Rotated Complementary H-Shaped Resonator Metasurface. *IEEE Transactions on Antennas and Propagation*, *65*(12), 7383–7388. doi:10.1109/TAP.2017.2763175

Hlali, A., Houaneb, Z., & Zairi, H. (2018). Dual-Band Reconfigurable Graphene-Based Patch Antenna in Terahertz Band: Design, Analysis and Modeling Using WCIP Method. *Progress In Electromagnetics Research C*, *87*, 213–226. doi:10.2528/PIERC18080107

Hlali, A., Houaneb, Z., & Zairi, H. (2019a). Tunable filter based on hybrid metal-graphene structures over an ultrawide terahertz band using an improved Wave Concept Iterative Process method. *International Journal for Light and Electron Optics*, *181*, 423–431. doi:10.1016/j.ijleo.2018.12.091

Hlali, A., Houaneb, Z., & Zairi, H. (2019b). Effective Modeling of Magnetized Graphene by the Wave Concept Iterative Process Method Using Boundary Conditions. *Progress In Electromagnetics Research C*, *89*, 121–132. doi:10.2528/PIERC18111514

Kianinejad, A., Chen, Z. N., & Qiu, Ch. W. (2015). Design and Modeling of Spoof Surface Plasmon Modes-Based Microwave Slow-Wave Transmission Line. *IEEE Transactions on Microwave Theory and Techniques*, *63*(6), 1817–1825. doi:10.1109/TMTT.2015.2422694

Kianinejad, A., Chen, Z. N., & Qiu, C.-W. (2018). Full Modeling, Loss Reduction, and Mutual Coupling Control of Spoof Surface Plasmon-Based Meander Slow Wave Transmission Lines. *IEEE Transactions on Microwave Theory and Techniques*, *66*(8), 3764–3772. doi:10.1109/TMTT.2018.2841857

Pozar, D. M. (2011). Microwave Engineering. John Wiley & Sons.

Tang, W. L., Zhang, H. Ch., Ma, H. F., Jiang, W. X., & Cui, T. J. (2019). Concept, Theory, Design, and Applications of Spoof Surface Plasmon Polaritons at Microwave Frequencies. *Advanced Optical Materials, 7*, 1–22.

Zhang, A. Q., Liu, Z. G., Lu, W. B., & Chen, H. (2019a). Dynamically Tunable Attenuator on a Graphene-Based Microstrip Line. *IEEE Transactions on Microwave Theory and Techniques*, *67*(2), 746–753. doi:10.1109/TMTT.2018.2885761

Zhang, A. Q., Liu, Z. G., Lu, W. B., & Chen, H. (2019b). Graphene-Based Dynamically Tunable Attenuator on a Coplanar Waveguide or a Slotline. *IEEE Transactions on Microwave Theory and Techniques*, *67*(1), 70–77. doi:10.1109/TMTT.2018.2875078

Zhang, A. Q., Lu, W. B., Liu, Z. G., Chen, H., & Huang, B. H. (2018). Dynamically Tunable Substrate Integrated Waveguide Attenuator Using Graphene. *IEEE Transactions on Microwave Theory and Techniques*, *66*(6), 3081–3089. doi:10.1109/TMTT.2018.2809577

Zhang, A. Q., Lu, W. B., Liu, Z. G., Wu, B., & Chen, H. (2019). Flexible and Dynamically Tunable Attenuator Based on Spoof Surface Plasmon Polaritons Waveguide Loaded With Graphene. *IEEE Transactions on Antennas and Propagation*, *67*(8), 5582–5589. doi:10.1109/TAP.2019.2911590

Zhang, X., Zhang, H. Ch., Tang, W. X., Liu, J. F., Fang, Z., Wu, J. W., & Cui, J. W. (2017). Loss Analysis and Engineering of Spoof Surface Plasmons Based on Circuit Topology. *IEEE Antennas and Wireless Propagation Letters*, *16*, 3204–3207. doi:10.1109/LAWP.2017.2768551

Chapter 10
Opportunity and Challenges for VLSI in IoT Application

Jyoti Kandpal
National Institute of Technology Arunachal Pradesh, India

Abhay Singh
https://orcid.org/0000-0003-4686-3795
G. B. Pant University of Agriculture and Technology, Pantnagar, India

ABSTRACT

Internet-of-things (IoT) systems combine sensing, computation, storage, and communication to sense physical systems and respond accordingly. However, larger size chips are not suitable for fog and edge devices. Therefore, a new mindset is required for VLSI design to implement the IoT application. This chapter describes the first conventional technology used in VLSI design. Afterward, the characteristics of IoT systems relevant to VLSI design identify essential factors and challenges at different levels. Finally, the fifth-generation network (5G) is also studied to expand IoT applications.

THE INTEGRATED CIRCUIT (I.C.) ERA

In the early 1900s, vacuum tubes were used to implement a large and bulky circuit to be used. In 1947, three physicists (Bardeen, Brattain, and Shockley) developed the first point-contact semiconductor transistor using germanium. Transistors are superior to conventional vacuum tubes in a smaller size, lower power, fast response time, and lower operating temperature. Jack Kilby introduced the first integrated

DOI: 10.4018/978-1-6684-3855-8.ch010

circuit (I.C.) in 1958. It was implemented on a 0.5-inch germanium bar with three resistors, a capacitor, and a transistor connected by platinum wire (Moore,1965).

MOORE'S LAW

Gordon Moore, the CEO of Fairchild Semiconductor and later co-founder of Intel, approximated the number of transistors in the chip based on the economics of the I.C.

Moore's First Law

In 1965, he predicted the IC would quadruple every year for the next decade. "The cost per component is nearly inversely related to the number of components," Moore states that having a larger number of transistors means a cheaper cost per transistor. He updated his forecast in 1975; the transistors count will double every two years. Moore's Law was frequently utilised from 1975 to 2015 to, forecast the number of transistors that could fit on a single integrated circuit with a high degree of precision. Moore's prediction for 1965-2020, is shown in Figure 1 below (Moore,1975; Borsuk & Coffey, 2003; Shalf, 2020).

The Second Law of Moore

While Moore's Law indicates that the cost of a computer (for customers) decreases as the number of components in an integrated circuit is increased, Moore's Second Law states that the capital cost of making IC increases significantly with time. Therefore, the prices of R&D, production, and testing rise considerably with each successive generation of chips (Mack, 2015).

Future, Moore's Law

Gordon Moore said in 2015, "Moore's Law appears to be approaching to an end as R&D expenditures rise and corporations reduce their rate of innovation. However, non-silicon computing, like AI-based chips, quantum computing and application-specific-integrated circuits (ASIC), is slowly gaining traction. Recent advancements in the computing trade could shortly result in significant efficiency benefits (Maekov, 2014; Colewell, 2013; International Technology Roadmap for Semiconductors [ITRS], 2011).

The Applications of Moore's Laws

The Law has been widely used in the semiconductor sector throughout the last five decades, resulting in significant economic, technological, and social benefits.

1. Moore's Law is utilised to set R&D goals and long-term production targets in the semiconductor business.
2. Moore law is used to develop digital electronics and introduce smaller, more powerful electronic devices.
3. It has reduced the cost of computing and made it more accessible, resulting in economic, societal and technological assistance.
4. It has maintained the semiconductor sector up to date with technical advancements, with practically every company adhering to the rule.

The semiconductor industry association (SIA) has periodically published a roadmap called the International Technology Roadmap for Semiconductors (ITRS) since 1993. The first edition of ITRS (1998-2013) highlighted the transistor density and the number of cores for the evolution of IC's, and the second edition of ITRS (ITRS 2.0) emphasized design and process technology (Meindl,1983).

For nearly three decades, the level of integration, as measured by the number of logic gates in a monolithic chip, has been continually increasing, owing to significant advances in interconnection and process technologies. The level of integration measures the complexity of the function. Even though more complicated operations are required in various telecommunications devices and data processing, the necessity to integrate these capabilities into a small package/system is growing. The evolution of logic complexity in integrated circuits during the preceding three decades is depicted in Table 1 (Nair, 2002; Nowak, 2002; Baccarani et al.,1984).

Table 1. Integration density of integrated circuit

Integration Level	Number of Transistors in a Chip	Year
Small scale integration (SSI)	<100	1950
Medium Scale Integration (MSI)	100 -1000	1960
Large Scale Integration (LSI)	1000 -10,000	1970
Very Large-Scale Integration (VLSI)	10,000 -1,00,000	1980
Ultra-Large-Scale Integration((ULSI)	1,00,000 -10,000,000	1990
Super Large-scale Integration (SLSI)	>10,000,000	Year

SCALING TECHNIQUES

Scaling techniques are used in CMOS and advanced technology to improve performance, increase the transistor density, and reduce power consumption. Dennard and Mead published a paper in the 1970s claiming that the basic MOS transistor architecture could be scaled down to smaller geometric parameters (Frank et al.,2001; Borkar,1999; Islam, 2015; Iaaac,1998; Skotnicki et al.,2005; Haron & Hamdioui, 2008; Tang, 1988).
There are three types of scaling methods which is described below:

1. Constant field scaling: In constant field scaling, the mounted devices are obtained by scaling all device voltages, dimensions of the transistor and the doping concentration densities by an aspect α
2. Constant Voltage scaling: The power supply (VDD) is kept constant while the process parameters scale down.
3. Lateral scaling: In lateral scaling, only the gate length is scaled. Therefore, it is also called "gate shrinking". The following points are concluded from the scaling.
    a. Reduction in the gate delay and increment in the maximum clock frequency;
    b. Device density is doubled;
    c. Reduction in the parasitic capacitance;
    d. Reduction in active power and energy per transition

TYPES OF PLANNER TECHNOLOGY

CMOS technology is the most common fabrication method for low-cost and high-performance VLSI circuits. Technology is continuously evolving to yield smaller systems with lower power dissipation. However, the I.C. industry is facing significant problems due to constraints on power density (W/cm^2), static power (standby) and high dynamic dissipation (operating). The key to overcoming these challenges lies in improvements in design, material and manufacturing processes. The evolution of MOSFET architectures is depicted in Figure 2, which shows double-gate, tri-gate, pi-gate, omega-gate, and gate-all-around. Due to its simple construction and ease of manufacture. Different types of planner technology are discussed (Doris et al., 2003; Lee et al.,1998).

1. Complementary Metal Oxide Semiconductor
2. SOI Based MOSFET
3. Double Gate MOSFET
4. Fin Field Effect Transistor (Fin FET)
5. CNTFET

Complementary Metal Oxide Semiconductor (CMOS)

Frank Wanlass and C.T.Sah designed the CMOS device in 1963, shown in Figure 3. To revolutionise the IC.,both p-MOS and n-MOS and transistors are fabricated on a similar wafer. The MOS transistor metal is used for gate material, SiO2 for insulator, and the substrate semiconductor. Different integrated circuits, microprocessors, microcontrollers, sensors, memory, and other digital circuits are implemented using CMOS technology. CMOS circuits reported low static power dissipation, high switching speed, and high integration density. These advantages encourage MOSFET downsizing and, as a result, the rapid development of high-density I.C. However, there is some limiting factor to scaling the MOS, which are as follows:

1. Quantum mechanical tunnelling includes gate, band-to-band and source to drain tunnelling.
2. Intrinsic parameter fluctuations
3. Higher power dissipation

Four different processes are used to fabricate the CMOS VLSI IC.

1. N-Well Process
2. P-Well Process
3. Silicon on Insulator (SOI) Process
4. Twin Tub Process

Demerit of MOS technology: The leakage current phenomenon become evident as the MOS device is scaled down.

SOI-Based MOSFET Structure

Mueller and Robinson presented the SOI transistor in 1964. The Silicon on Insulator (SOI) features low capacitance technology, allowing it to operate at high speeds. In addition, by lowering the power supply, power consumption is reduced while adequate speed is maintained. However, the benefits of SOI technology extend beyond speed and power; they also include the capacity to handle high voltage and tolerate extreme temperatures. In this design, a thin layer of about tens of nanometer active silicon is placed on top of a thick layer of an insulator such as silicon dioxide (SiO_2)-sometimes referred to as Buried Oxide (BOX)- shown in figure 4.This type of arrangement reduces the internal junction capacitance and parasitic capacitance. Therefore, device performance by a significant percentage is improved (Kilchytska, 2011; Nikonov & Young, 2016; Liu, 2012).

In bulk CMOS, leakage current passes through the substrate, while in SOI CMOS, leakage current does not flow through the substrate. As a result, depending on the operating mode, two categories of SOI MOSFETs are presented: fully depleted SOI MOSFET and partially depleted SOI MOSFET (PDSOI) (Flandre et al.,1999; Taur et al.,1997).

Merits

1. Silicon Channel layer is grown on a layer of oxide.
2. Absence of junction capacitance.
3. Low leakage current and compatible fabrication technology
4. Reduced parasitic effects
5. Absence of latch-up problem
6. Reduction in leakage

Demerits

1. Drain current overshoot
2. Kink effect
3. Thickness control

Double Gate (D.G.) MOSFET Technology

When conventional MOSFET technology became harder to scale down in size, DG MOSFET technology was invented. DG MOSFET is implemented when the gate length L_g<50nm. The gate coupling effect provides a lower threshold voltage (V_{th})

and a higher on/off current ratio. Figure 5 represent the DG MOSFET implementation (Zhang, 2010; Kararia & Beniwal, 2016).

Features

1. Upper and Lower gates control the channel region.
2. Directly scalable down to 20 nm Channel length.
3. Ultra-thin body as a rectangular quantum well at device limits.
4. Improved subthreshold slope

Merits

1. Short channel effect control: Better scalability & lower DIBL
2. High Drive current
3. Near ideal sub-threshold slope
4. Lower Gate leakage and sub-threshold current
5. Elimination of V_t variation due to random dopant fluctuation

Demerits

1. The standard fabrication process is needed for the fabrication
2. Maintaining a thin, consistent channel thickness is a significant challenge.

Fin Field Effect Transistor (Fin FET)

A FinFET transistor is implemented on SOI substrate in which gates are positioned on the two, three and four sides of the channel. This implementation source/drain form of fins on the silicon surface is shown in Figure 6 (Pal et al., 2017; Liu, 2012; Dang et al.,2006).

Merits

1. This structure is a quasi-planner.
2. This structure has a high drive current.
3. Suitable for SRAM implementation.
4. Faster switching time due to extensive current drive capability.

Demerits

1. Fabrication of FinFet is complex.
2. Higher parasitic capacitance due to 3D profile
3. Fabrication cost is higher.
4. Corner effects

Carbon Nanotube FET

Japanese physicist S. Iijima invented the carbon nanotube in 1991, shown in figure 7. CNT is a nanoscale tube made up of rolled sheets of graphene. There are two types of CNT structures: single-walled (SWCNT) and multi-walled (MWCNT). SWCNT consists of a single nanotube, whereas MWCNT comprises multiple nanotubes with an interlayer spacing of 0.34 nm. CNTFET is also a four-terminal device. The channel region of the device consists of undoped nanotubes, which are semiconducting, and are placed in the channel region beneath the gate. In contrast, the highly doped nanotubes are placed between the drain/source and the gate terminals. Therefore, this structure reported smaller dimensions and higher electron mobilities (Zahoor et al., 2021; Sepranos & Wolf, 2019).

Merits

1. Higher current density
2. Higher Threshold slope
3. Better control over channel
4. Higher electron mobility

Demerits

1. Production cost is higher
2. Reliability issue, the failure rate is higher than CMOS

The most challenging issue is to reduce the contact resistance between the nanodevice and the external world, which is 6Kohm. In addition, a cost-effective manufacturing process will have to be developed for the mass production of CNTFET.

INTERNET OF THINGS (IOT)

Beyond the 28nm (feature size), scaling became tremendously tedious due to double lithography and FinFET structure in the absence of lithographic scaling. Therefore, there are several additional methods for maintaining performance scaling. These methods are divided into three strategies for scaling beyond the lithographic scaling and to obtain further performance improvement. The First method emphasizes advanced packaging technologies and specialized architecture. The second method represents emerging CMOS-based devices and transistors that will enhance performance. Finally, the third method proposed new models for computation- and solved problems like quantum computing (Fuqaha, 2015; Khan & Salah, 2018).

A system in package configuration often requires a combination of mature manufacturing nodes and novel technologies for sensing, low power operation, communication and computation. Therefore, VLSI devices are used in IoT systems for wide applications like medicine, energy, transportation, and smart homes. In conventional chip systems, large chips are used; however, IoT device design highlights low power consumption and low cost (I. Lee & K. Lee, 2015; Gubbi et al.,2013).

IoT connects millions of autonomous devices to the internet. These devices collect physical parameters and processes and report those to the network. In addition, some autonomously or network commands provide outputs that control other equipment and systems. There is a wide range of applications for IoT devices, including infrastructure, utilities, home automation, personal medical, vehicle, industrial, and more. According to IDC (tech analyst), there will be 41.6 billion connected IoT devices or things by 2025. The market for IoT devices will explode as additional applications are addressed (Madakam et al.,2015; Mahmoud et al.,2015; Chen et al.,2014).

Figure 8 presents the block diagram of IoT, and it contains the four components:

1. **Sensors:** IoT devices take the input using the sensors, miniaturised through MEMS technology. Afterwards, this information is sent out through wired or wireless interfaces to mobile and cloud computers.
2. **Gateways:** Cellular networks, Wi-Fi, satellite networks, Bluetooth (WAN), low-power vast area networks, wide-area networks and other communication & transport methods connect the sensors to the cloud.
3. **Cloud/Server:** The acquired data is processed by the software.
4. **User interface:** The data is made available to the end-user. This can be accomplished by setting alerts on their phones or sending them emails and messages.

VLSI designers have an incredible prospect to design even smaller chips to address a wide range of needs using mature and emerging technology in IoT systems. IoT provides a platform for connecting 50 billion devices in a 5G network by 2030, with a download speed of 2.4 Gbps
Following Advantages of IoT application are reported:

1. Monitor Data
2. Ease of Access
3. Speedy Operation
4. Adapting to new standards
5. Better time management
6. Automation and control

Though the IoT has a lot of advantages, it also has a lot of drawbacks. Here's a list of some of the biggest concerns:

1. **Security:** IoT creates an ecosystem of constantly connected devices communicating over networks. Due to limited controlling techniques, the systems are vulnerable to different attackers.
2. **Privacy –**Without the user's direct participation, the sophistication of IoT offers essential personal data in extreme detail.
3. **Complexity –** IoT systems are challenging to design, install, and maintain.
4. **Flexibility –**IoT systems do not readily interact with another system.

The IoT combines a diffuse layer of devices, sensors, and computing power that intersect entire consumer, business-to-business, and government industries (Farooq et al.,2015; Nord et al.,2019; Benini & Micheli, 2002).

As a result, estimates for IoT market value are massive. The government and top business-to-business applications are described in the following section:

1. **Connected advertising and Marketing**: Along with intelligent manufacturing and telecommuting support systems, Cisco predicts this category (for example, Internet-connected billboards) will be one of the top three IoT categories.
2. **Intelligent traffic management system**: According to GSM association, research estimates $100 billion in revenue will be generated by 2020 for applications such as toll-taking and congestion charges. Innovative parking-space management, which is predicted to develop $30 billion in revenue, is a related revenue stream.
3. **Waste management system:** In Cincinnati, a "pay as you trash" programme that employed IoT technology to monitor people who exceeded waste limitations

resulted in a 17 per cent decrease in household waste volume and a 49 per cent increase in recycling volume.

4. **Smart electricity grid that adjusts rate for peak energy usage**: According to the McKinsey Global Institute, these savings will amount to $200 billion to $500 billion per year by 2025.
5. **Innovative water system and meters:** By installing a sensor on pumps and other water infrastructure, Doha Paulo and Beijing have decreased leakage by 40 to 50 per cent.
6. **Industrial uses:** It includes an internet-controlled production line, linked factories and warehouse.

Benefits of IoT to Organization

1. Save money and time.
2. Boost employee efficiency.
3. Adapt and integrate business models.
4. Make sensible business strategies.
5. Increase your profits.

SYSTEM ON CHIP (SOC)

System on a Chip technology is employed in embedded systems and general-purpose computing devices across all industries. According to research, the system on a Chip market would reach $207 billion by 2023. The SoC technology improves on the traditional system architecture approach, in which each component is put separately (for example, on motherboards). This permits the development of smaller, more efficient devices, propelling innovation in the development of netbooks, laptops, smartphones, and IoT devices. An SoC is a single integrated circuit containing all of the compounds in a modern computer system. A CPU (Central Processing Unit), storage, I/O (input/output) ports, RAM (Random Access Memory), and other components are placed on an SoC. An SoC strives for efficiency in power consumption and in size (Chakravarthi,2019; Ishtiaq et al.,2021; Ko, 2016; Wu et al.,2018).

Different Types of SoC

The SoC can be implemented in a variety of ways. Therefore, we looked at many sorts of SoCs in the following section.

1. SoCs that uses Microprocessor

One of the most popular SoCs with microprocessors is Qualcomm's Snapdragon. Qualcomm's Kryo 485 processor powers the Snapdragon 855+ platform. A Wi-Fi 6 features, GPU (Graphics Processing Unit), an LTE modem, a camera and USB-C functionality determine the Kryo 485's computing power. Mobile phones, tablets, and other sophisticated devices frequently contain these processors. These microprocessors were favored because of their low power consumption and excellent computing capacity; as a result, they were able to optimize functionality while maintaining a small footprint.

2. SoCs that use Microcontroller

The peripherals that can be used with a microcontroller are limited compared to those interfaced with SoC. Therefore, a microcontroller does not typically provide the same level of capability as an SoC. For example, while an SoC can run an operating system on an intelligent device as a whole, microcontrollers typically run a single programme. Nevertheless, microcontrollers are widely employed as SoC components. The CC2540 from Texas Instruments, for example, is based on the 8051 microcontrollers. With functionalities that include in-system programmable flash, RAM, Bluetooth capabilities, and more, the CC2540 expands the potential of the 8051. Microcontroller-based SoCs like the CC2540 is vital in driving embedded system growth.

3. Applications for ASIC (Application-Specific Integrated Circuit)

SoC supports general-purpose computing for mobile devices, and Application-Specific Integrated Circuit (ASIC) is designed to carry out a specific task instead of general-purpose computing. In the embedded systems industry, purpose-built applications are quite common. According to Semico's research, the ASIC/SoC market is expected to develop at a robust 5.5 per cent Compound Annual Growth Rate (CAGR) through 2025. IoT and Artificial Intelligence (A.I.) are the key drivers of the ASIC/SoC market growth (Semica Research Corporation, 2022).

To provide the highest integration and management of the area, the new IoT inventions are implemented with a single system on a chip (SoC). With applications ranging from IoT in healthcare to intelligent home technology, the potential use cases for SoC appear to be practically unlimited. Smartphones, tablets, netbooks and other smart gadgets are among the most common applications for SoC. These devices show how SoC may give significant general-purpose computing functionality while consuming less power and taking up less space.

Many factors must be considered when designing a custom SoC for IoT applications. These factors include device size, power consumption, latency, and data throughput. The data rate, range and power are the three most significant considerations. These parameters are interrelated. Data rate and data range depend on protocol.

The IoT SoC block diagram is shown in figure 9. The functional blocks employed in a typical SoC are either standardised or substantially commoditised at the bottom portion of the diagram. Using commercially provided I.P. blocks for these functions reported several benefits in terms of power and latency. The low power wireless SoC for IoT applications are frequently tuned for battery-operated sensors like those found in smart door locks, smart thermostats, etc. Furthermore, the SoC with built-in wireless communication features typically uses power-saving algorithms that allow them to require only a few microamperes, substantially prolonging the battery life further.

Most IoT SoC applications are developed in small geometry (less than or equal to 55 nm) to maximise power and area-saving on the die on which they are built. However, analogue circuit design presents significant challenges in small process implementation due to transistor mismatch and leakage. Vidatronic (PMU) allows overcoming the difficulties of methods in progressively smaller size down to 7nm.

IoT SoCs structure consists of the following blocks:

1. A low-dropout regulator built on-die provides the varied voltage rails required on the SoC without an external component.
2. DC-to-DC converters generate the necessary output voltage if the input voltage is above or below the required output voltage.
3. Voltage references are used for various op-amps, comparators, data converters, and other analogue and mixed-signal functions. Three desired characteristics in a voltage reference include low power consumption, high accuracy and good power supply noise rejection.
4. Comparators, op-amps, analogue, mixed-signal functions, and data converters use voltage references. Excellent accuracy, low power consumption, high accuracy and noise rejection are three desirable properties in a voltage reference.
5. Fundamental logic blocks
6. Serial interfaces and Control logic.

Vidatronic can also adapt any I.P. block to satisfy specific application needs and merge the essential blocks into a complete Power Management Unit that handles all of your SoC's power needs. Vidatronic emphasizes CMOS, SOI and FinFET planar technologies as we move from 180 nm to 7 nm process technology (Brittany Torres, 2021).

Most IoT gadgets are battery-operated and have a finite amount of energy. Context inference apps' algorithms, such as feature calculations and classifications, are power-intensive and computational. They frequently need to run in the background to provide just-in-time feedback, notifications, and interventions. Most always-on context inferences are now run on the device's primary app processor, which accounts for a large amount of the device's overall workload and energy consumption. The addition of power-hungry sensors like GPS and cellular radio frequently exacerbates this high-power usage. The following part considers both device and processor heterogeneity to enhance the context inferences' energy efficiency and accuracy in IoT devices (Vargas et al.,2016).

1. Device Heterogeneity

Today's commercial off-the-shelf (COTS) smartwatches like the Moto 360 (Android) and Apple Watch (iOS) are employed with robust system hardware such as RAM and CPUs that are comparable to those found in modern smartphones. These wearables can operate as user portals for standalone host apps or smartphone apps due to their efficient Bluetooth low Energy (BLE) connectivity to phones. These devices also have many sensors that can facilitate context inferences. Because of their small weight, they are perfect for continuous context monitoring. Furthermore, watches are less intrusive than phones since they are less likely to disrupt a user's daily routine while worn. Sensing and inference workloads can be swapped between available devices at any time for enhanced sensor coverage and inference accuracy by coordinating smartwatches and smartphones. We achieved up to a 37 per cent improvement in inference accuracy and a 61 per cent reduction in energy usage by using a phone and watch for inference executions (Akpakwu et al.,2017).

2. Processor Heterogeneity

Modern mobile processors such as the Qualcomm Snapdragon are sophisticated systems on chip (SoCs), where heterogeneous coprocessors complement the leading app processors. As a result, energy efficiency is improved by shifting processing from the central app processor (CPU) to a secondary low-power processor. Mobile chip vendors have commenced efforts to make these previously hidden coprocessors, such as the digital signal processor (DSP), programmable. For example, the Hexagon 680 DSP of the Snapdragon 820 series SoC can be custom-programmed and runs in the ultra-low-power range. Offloading the classification stage commonly seen in an inference pipeline to DSP results in up to 60 per cent energy savings with negligible latency effects.

3. IoT Device Heterogeneity

Table 1 compares the hardware specs of prominent smartphones and smartwatches to validate the benefits of the user device and CPU heterogeneity. Smartwatches now have substantial RAM, CPUs, and radios, allowing them to run standalone apps without the need for a smartphone. The Moto 360 and Apple Watch have sensors and radios similar to those found in today's smartphones, including optical heart-rate sensors. On the other hand, smartwatches have a significantly smaller battery capacity than smartphones due to space and weight restrictions. We chose the Moto 360 as an example platform to assess our app scenarios because of the wearable hardware similarities (Table 2). We generated basic power profiles of a Moto 360 watch and a Nexus 5 phone to investigate further the viability of running context inferences on smartwatches (Table 3). We analysed the power consumption of the watch and the phone while BLE connected and profiled both devices for screen off (sleeping) and screen on because their typical power usage is somewhere in the middle. Compared to the Nexus 5 smartphone, the Moto 360 watch consumes less power. On the watch, however, the power differential between screen off and screen on is considerably greater than on the phone, necessitating a thorough examination of the power and energy tradeoffs of inference operations.

Table 2. Comparative analysis of hardware platforms

Gadget	System on Chip (SoC)	CPU	RAM	Storage	Radio	Battery	Weight	Sensors
Apple Watch	Apple S1	520 MHz S1	512 MBytes	8Gbytes	Near field communication (NFC)/ BLE/ Wi-Fi/	3.8V 205mAh	25g	Accelerometer, Pedometer, Heartrate, Gyroscope, microphone
Moto 360 Watch	TI OMAP3630	1GHz OMAP3	512 MBytes	4Gbytes	Wi-Fi/ BLE	3.8V 320mAh	49g	Accelerometer, Pedometer, Heartrate, Gyroscope, light, Microphone
Nexus 5Phone	Snapdragon 800	2.3GHz Krait	2GBytes	16/32Gbytes	NFC/ BLE/ WiFi/	4.3V 2300mAh	130g	Accelerometer, Pedometer, ,light,GPS, Gyroscope, Heartrate, Microphone

Table 3. Competitive analysis of different parameters electronics gadgets

Gadgets	Power(W)	Current(mA)	Duration of Life(h)
Moto360 watch (screen off)	0.13	3.283	97.472
Moto360 watch (screen on)	0.550	142.520	2.245
Nexus 5phone (screen off)	0.254	58.913	37.343
Nexus 5phone (screen on)	1.853	435.260	5.057

FIFTH GENERATION (5G) APPLICATION

Several wireless technologies, like second-generation(2G) / Third Generation(3G) / fourth-generation (4G), Bluetooth, and Wi-Fi, have been employed in heterogeneous IoT applications, in which wireless communication technologies will connect billions of devices (Li et al.,2018; Fuqaha et al.,2015).

2G networks (which presently cover 90% of the world's population) are built for voice, 3G networks (which currently cover 65 per cent of the world's population) are designed for voice plus data, and 4G networks (which have been available since 2012) are designed for broadband internet experiences. IoT is widely used, although 3G and 4G are not fully optimised for IoT applications. The capabilities of cellular networks that can give usable Internet connectivity to IoT devices have substantially improved thanks to 4G. In comparison to rival technologies such as BLE (Mackensen et al.,2012) WiMAX (Zemrane et al.,2018)) ZigBee (Ergen, 2004; Taylor,2011), SigFox (Gomez et al.,2019), LoRa (Bor et al.,2016, Vangelista et al.,2015), the long-term evolution (LTE) to 4G connectivity has become the fastest and most consistent type of 4G since 2012 (Oyj, 2016).

Increased demand from consumers and businesses and more affordable devices are required for 5G and IoT adoption. Furthermore, spectrum and infrastructure and the worldwide standard's deployment are assisting in driving growth and increasing market interest in the IoT.

The majority of 5G application cases fall into one of three categories:

1. Mobile Broadband Enhancement
2. Massive Internet of Things
3. Communication

Self-driving cars, smart energy grids, better factory automation, and other demanding applications will become a reality thanks to 5G's ultra-reliability and low latency. In addition, as 5G increases network capacity, cloud computing, artificial intelligence, and edge computing, these capabilities will aid in handling the data quantities created by the IoT. Additional 5G innovations, such as network slicing, non-public networks, and 5G core, will eventually aid in the realization of the goal of a worldwide IoT network that can handle a large number of connected devices. According to GSMA Intelligence, IoT connections will reach 25.2 billion by 2025. According to the report, cellular technologies, such as low-power wide-area mobile IoT networks, would be used by 3.1 billion of these devices. Wireless technologies are used in today's IoT devices in various ways. For example, short-range technologies, such as Wi-Fi, Bluetooth, ZigBee, and Z-wave, often use unlicensed spectrum, while wide-area cellular technologies, such as GSM, LTE, and 5G, use licensed spectrum.

Low-power technologies operating in unlicensed spectra, such as LoRa and Sigfox, are alternatives. However, enhanced provisioning, device management, and service enablement are advantages of cellular technologies working in a licensed range for IoT devices. Furthermore, cellular networks provide worldwide coverage high levels of reliability, security, and performance that even the most demanding IoT applications require. Today's 5G networks are built on 4G networks that use both LTE for Machines (LTE-M) and Narrowband-IoT (NB-IoT) technologies, with 5G providing the capabilities needed to serve both current and future use cases (Nolan, 2018; Bangerter et al.,2014; Adimulam & Srinivas, 2017).

5G offers several advantages to the Internet of Things that aren't available with 4G or other technologies. 5G's capacity to serve many static and mobile IoT devices with varying speed, bandwidth, and quality of service requirements is one of them. The majority fall into three categories: improved mobile broadband (eMBB), massive IoT (mMTC), or vital communications.

The GSMA anticipates 5G to deliver high-speed, low-latency, dependable, and secure mobile broadband in its early deployments. In addition, massive numbers of IoT devices will eventually be connected to 5G networks, allowing for ultra-reliable and low-latency communications (Calhoum & Wentzloff, 2015; Wang et al.,2018; Goudos et al.,2017; Zhong et al.,2019; Bharathi et al.,2021; Yasemin et al.,2022). The 5G network delivers the following improvement:

1. Reduced latency
2. Increased density
3. Increased spectrum efficiency
4. Increased traffic capacity
5. Increased network efficiency

CONCLUSION

This chapter discussed the importance of Moore's law and the International Technology Roadmap for Semiconductor Technology. Moore's law and the ITRS have contributed significantly to the evolution of CMOS technology and development for next-generation devices. After then, the advantages and disadvantages of each planar technique are examined.

VLSI designers have a lot of opportunities with the Internet of things. The IoT industry provides a chance to implement the smaller chips to address a wide range of markets. In addition, mature and upcoming technologies are combined using either process or package methods to offer innovative capabilities.

The successful implementation of the VLSI IoT system requires different combinations of sensing, processing, storage, and communication devices according to the application. Afterwards, this chapter also covers the recent research work, challenges and trends on the 5G network.

REFERENCES

Adimulam, M. K., & Srinivas, M. B. (2017, November). Ultra-low power programmable wireless exg soc design for iot healthcare system. In *International Conference on Wireless Mobile Communication and Healthcare* (pp. 41-49). Springer.

Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5G networks for the Internet of Things: Communication technologies and challenges. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 3619–3647.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376.

ASIC design starts for 2022 by Key End Market Applications. (2022). Retrieved February 10, 2022 from https://semico.com/content/asic-design-starts-2022-key-end-market-applications

Baccarani, G., Wordeman, M. R., & Dennard, R. H. (1984). Generalized scaling theory and its application to a 1/4 micrometer MOSFET design. *IEEE Transactions on Electron Devices*, *31*(4), 452–462.

Benini, L., & De Micheli, G. (2002). Networks on chips: A new SoC paradigm. *Computer, 35*(1), 70-78.

Bharathi, N., & Jayavel, K. (2021, December). Role of VLSI Design To Build Trusted And Secured IOT Devices-A Methodological Approach. In *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 473-479). IEEE.

Bor, M., Vidler, J. E., & Roedig, U. (2016). *LoRa for the Internet of Things*. Academic Press.

Borkar, S. (1999). Design challenges of technology scaling. *IEEE Micro*, *19*(4), 23–29.

Borsuk, G. M., & Coffey, T. (2003). Moore's Law: a department of defense perspective (No. 30). Center for Technology and National Security Policy, National Defense University.

Calhoun, B. H., & Wentzloff, D. D. (2015, August). Ultra-low power wireless SoCs enabling a batteryless IoT. In *Hot Chips Symposium* (pp. 1-45). Academic Press.

Chakravarthi, V. S. (2019). *A Practical Approach to VLSI System on Chip (SoC) Design: A Comprehensive Guide*. Springer Nature.

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 Journal, 1*(4), 349-359.

Chih-Tang, S. (1988). Evolution of the MOS transistor-from conception to VLSI. *Proceedings of the IEEE*, *76*(10), 1280–1326.

Colwell, R. (2013, August). The chip design game at the end of Moore's law. In *2013 IEEE Hot Chips 25 Symposium (HCS)* (pp. 1-16). IEEE Computer Society.

Dang, T., Anghel, L., & Leveugle, R. (2006, September). Cntfet basics and simulation. In *International Conference on Design and Test of Integrated Systems in Nanoscale Technology, 2006. DTIS 2006.* (pp. 28-33). IEEE.

Doris, B., Ieong, M., Zhu, T., Zhang, Y., Steen, M., Natzle, W., . . . Haensch, W. (2003, December). Device design considerations for ultra-thin SOI MOSFETs. In *IEEE International Electron Devices Meeting 2003* (pp. 27-3). IEEE.

Ergen, S. C. (2004). *ZigBee/IEEE 802.15. 4 Summary.* UC Berkeley.

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *International Journal of Computers and Applications*, *113*(1), 1–7.

Flandre, D., Colinge, J. P., Chen, J., De Ceuster, D., Eggermont, J. P., Ferreira, L., ... Silveira, F. (1999). Fully-depleted SOI CMOS technology for low-voltage low-power mixed digital/analog/microwave circuits. *Analog Integrated Circuits and Signal Processing*, *21*(3), 213–228.

Frank, D. J., Dennard, R. H., Nowak, E., Solomon, P. M., Taur, Y., & Wong, H. S. P. (2001). Device scaling limits of Si MOSFETs and their application dependencies. *Proceedings of the IEEE*, *89*(3), 259–288.

Gomez, C., Veras, J. C., Vidal, R., Casals, L., & Paradells, J. (2019). A sigfox energy consumption model. *Sensors (Basel)*, *19*(3), 681.

Goudos, S. K., Dallas, P. I., Chatziefthymiou, S., & Kyriazakos, S. (2017). A survey of IoT key enabling and future technologies: 5G, mobile IoT, sematic web and applications. *Wireless Personal Communications*, *97*(2), 1645–1675.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectureal elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Haron, N. Z., & Hamdioui, S. (2008, December). Why is CMOS scaling coming to an END? In *2008 3rd International Design and Test Workshop* (pp. 98-103). IEEE.

International Technology Roadmap for Semiconductors. (2011). Retrieved December 12, 2021, from http://www.itrs.net/

Isaac, R. D. (1998, October). Reaching the limits of CMOS technology. In *IEEE 7th Topical Meeting on Electrical Performance of Electronic Packaging* (p. 3). IEEE.

Ishtiaq, A., Khan, M. U., Ali, S. Z., Habib, K., Samer, S., & Hafeez, E. (2021, August). A Review of System on Chip (SOC) Applications in Internet of Things (IOT) and Medical. In *ICAME21, International Conference on Advances in Mechanical Engineering* (pp. 1-10). Academic Press.

Islam, A. (2015, June). Technology scaling and its side effects. In *2015 19th International Symposium on VLSI Design and Test (VDAT)* (pp. 1-1). IEEE Computer Society.

Kataria, S., & Beniwal, P. (2016). FinFET Technology: A Review Paper. *International Journal of Technical Research*, *5*(2).

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411.

Kilchytska, V., Andrieu, F., Faynot, O., & Flandre, D. (2011, March). High-temperature perspectives of UTB SOI MOSFETs. In *Ulis 2011 Ultimate Integration on Silicon* (pp. 1–4). IEEE.

Ko, U. (2016, April). Ultra-low power SoC for wearable & IoT. In *2016 International Symposium on VLSI Technology, Systems and Application (VLSI-TSA)* (pp. 1-1). IEEE.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440.

Lee, J. W., Kim, H. K., Oh, J. H., Yang, J. W., Lee, W. C., Kim, J. S., ... Koh, Y. H. (1998, October). A new SOI MOSFET for low power applications. In *1998 IEEE International SOI Conference Proceedings (Cat No. 98CH36199)* (pp. 65-66). IEEE.

Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, *10*, 1–9.

Liu, T. J. K. (2012). Introduction to multi-gate MOSFETs. *6th Annual SOI Fundamentals Class, 3*.

Liu, T. K. (2012, June). FinFET history, fundamentals and future. In *Proceedings of the Symposium on VLSI Technology Short Course*. University of California

Mack, C. (2015). The multiple lives of Moore's law. *IEEE Spectrum*, *52*(4), 31–31.

Mackensen, E., Lai, M., & Wendt, T. M. (2012, October). Bluetooth Low Energy (BLE) based wireless sensors. In SENSORS, 2012 IEEE (pp. 1-4). IEEE.

Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(05), 164.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336-341). IEEE.

Markov, I. L. (2014). Limits on fundamental limits to computation. *Nature*, *512*(7513), 147–154.

Meindl, J. D. (1983, December). Theoretical, practical and analogical limits in ULSI. In *1983 International Electron Devices Meeting* (pp. 8-13). IEEE.

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics (Basel)*, *38*(8).

Moore, G. E. (1975, December). Progress in digital integrated electronics. In Electron devices meeting (Vol. 21, pp. 11-13). Academic Press.

Nair, R. (2002). Effect of increasing chip density on the evolution of computer architectures. *IBM Journal of Research and Development, 46*(2.3), 223-234.

Nikonov, D. E., & Young, I. A. (2013). Overview of beyond-CMOS devices and a uniform methodology for their benchmarking. *Proceedings of the IEEE*, *101*(12), 2498–2533.

Nolan, S. M. (2018). Power Management for Internet of Things (IoT) System on a Chip (SoC). *Development.*

Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, *133*, 97–108.

Nowak, E. J. (2002). Maintaining the benefits of CMOS scaling when scaling bogs down. *IBM Journal of Research and Development, 46*(2.3), 169-180.

Oyj, N. (2016). *LTE evolution for IoT connectivity.* Nokia Corporation White Paper.

Pal, R. S., Sharma, S., & Dasgupta, S. (2017, March). Recent trend of FinFET devices and its challenges: A review. In *2017 Conference on Emerging Devices and Smart Systems (ICEDSS)* (pp. 150-154). IEEE.

Sepranos, D., & Wolf, M. (2019). Challenges and Opportunities in VLSI IoT Devices and Systems. *IEEE Design & Test*, *36*(4), 24–30.

Shalf, J. (2020). The future of computing beyond Moore's law. *Philosophical Transactions of the Royal Society A*, *378*(2166), 20190061.

Skotnicki, T., Hutchby, J. A., King, T. J., Wong, H. S., & Boeuf, F. (2005). The end of CMOS scaling: Toward the introduction of new materials and structural changes to improve MOSFET performance. *IEEE Circuits and Devices Magazine*, *21*(1), 16–26.

Taur, Y., Buchanan, D. A., Chen, W., Frank, D. J., Ismail, K. E., Lo, S. H., ... Wong, H. S. (1997). CMOS scaling into the nanometer regime. *Proceedings of the IEEE*, *85*(4), 486–504.

Taylor, L. (2011, October). Alliance, and Zig Bee, Interconnecting ZigBee & M2M networks. In *Proc. ETSI M2M Workshop* (pp. 1-18). Academic Press.

Vangelista, L., Zanella, A., & Zorzi, M. (2015, September). Long-range IoT technologies: The dawn of LoRa. In *Future access enablers of ubiquitous and intelligent infrastructures* (pp. 51–58). Springer.

Vargas, D. C. Y., & Salvador, C. E. P. (2016). Smart IoT gateway for heterogeneous devices interoperability. *IEEE Latin America Transactions*, *14*(8), 3900–3906.

Vidatronic Announces Series of Integrated Power Management Unit (PMU) IP Cores Optimized for Augmented/Virtual Reality Applications. (2021) Retrieved December 10, 2021 from https://www.vidatronic.com/vidatronic-announces-series-of-integrated-power-management-unit-pmu-ip-cores-optimized-for-augmented-virtual-reality-applications/

Wang, D., Chen, D., Song, B., Guizani, N., Yu, X., & Du, X. (2018). From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies. *IEEE Communications Magazine*, *56*(10), 114–120.

Wu, C. Y., Lou, J. C., & Deng, Z. B. (2018, April). An ultra-low power capacitor-less LDO for always-on domain in NB-IoT applications. In *2018 IEEE International Conference on Applied System Invention (ICASI)* (pp. 137-140). IEEE.

Yesmin, T., Agasti, S., & Chakrabarti, K. (2022). 5G Security and Privacy Issues: A Perspective View. In *ICT with Intelligent Applications* (pp. 89–98). Springer.

Zahoor, F., Hussin, F. A., Khanday, F. A., Ahmad, M. R., Mohd Nawi, I., Ooi, C. Y., & Rokhani, F. Z. (2021). Carbon nanotube field effect transistor (cntfet) and resistive random-access memory (rram) based ternary combinational logic circuits. *Electronics (Basel)*, *10*(1), 79.

Zemrane, H., Abbou, A. N., Baddi, Y., & Hasbi, A. (2018, November). Wireless Sensor Networks as part of IOT: Performance study of WiMax-Mobil protocol. In *2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)* (pp. 1-8). IEEE.

Zhang, L., Chan, M., & He, F. (2010, December). The impact of device parameter variation on double gate tunneling FET and double gate MOSFET. In *2010 IEEE International Conference of Electron Devices and Solid-State Circuits (EDSSC)* (pp. 1-4). IEEE.

Zhong, M., Yang, Y., Yao, H., Fu, X., Dobre, O. A., & Postolache, O. (2019). 5G and IoT: Towards a new era of communications and measurements. *IEEE Instrumentation & Measurement Magazine*, *22*(6), 18–26.

APPENDIX

Figure 1.

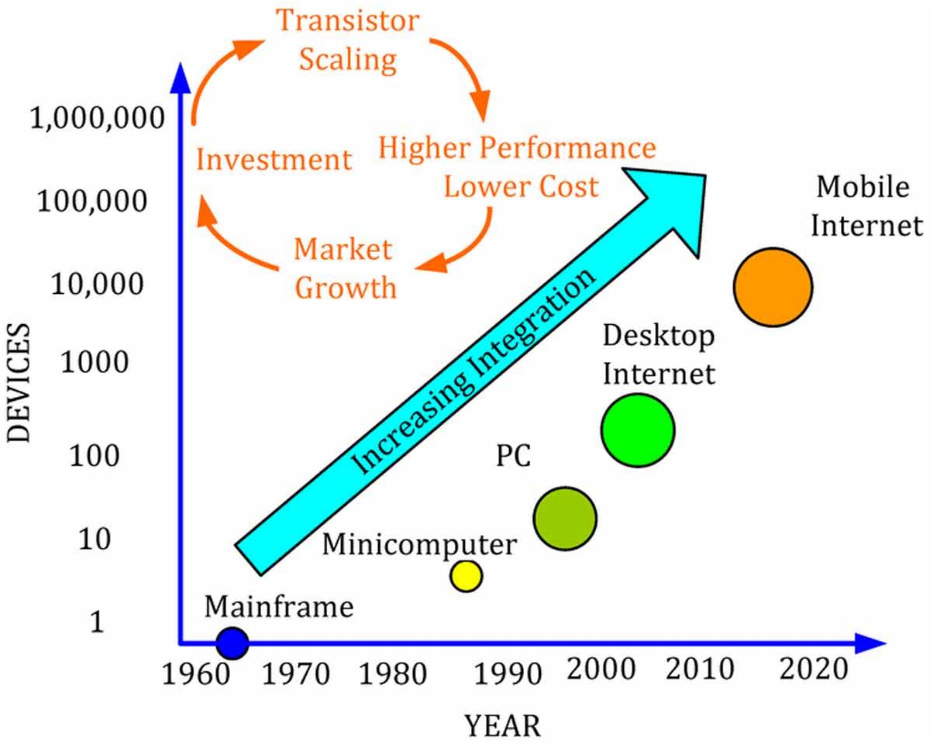


Figure 2.

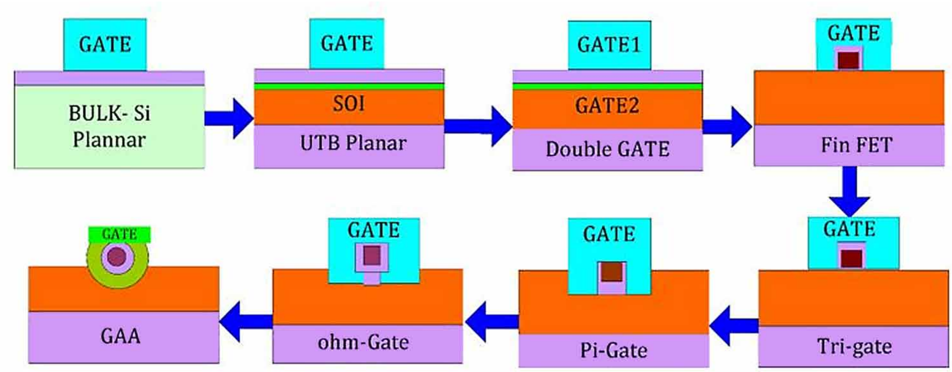


Figure 3.

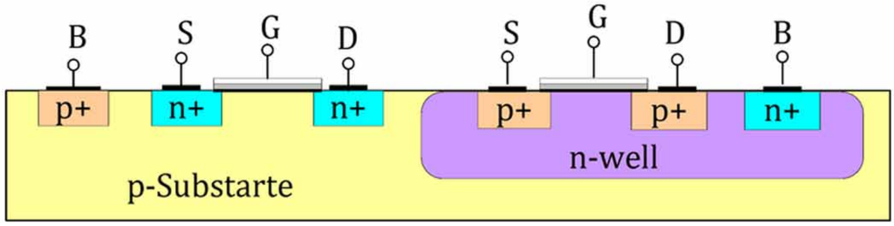


Figure 4.

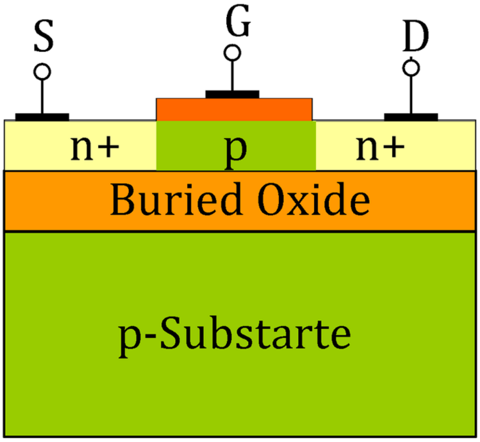


Figure 5.

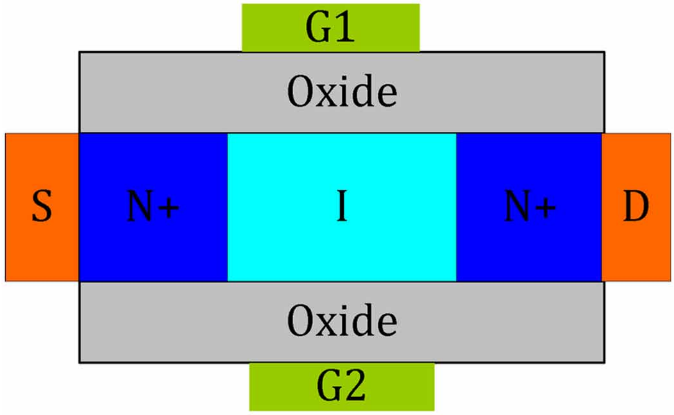


Figure 6.

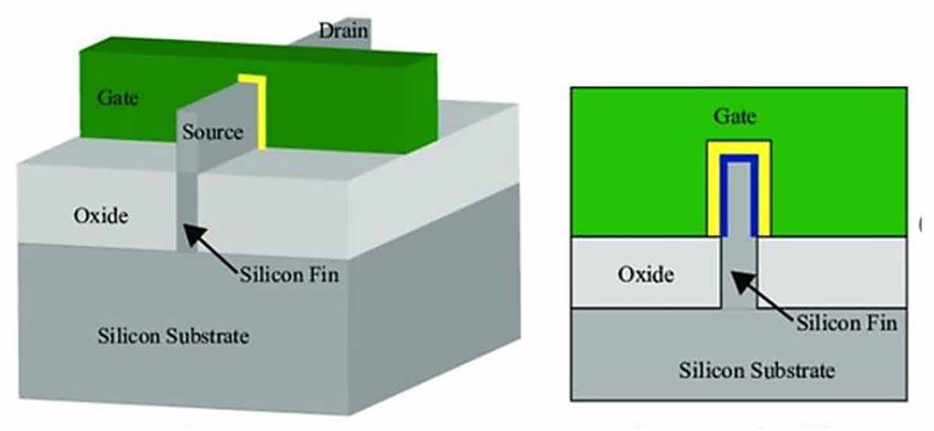


Figure 7.

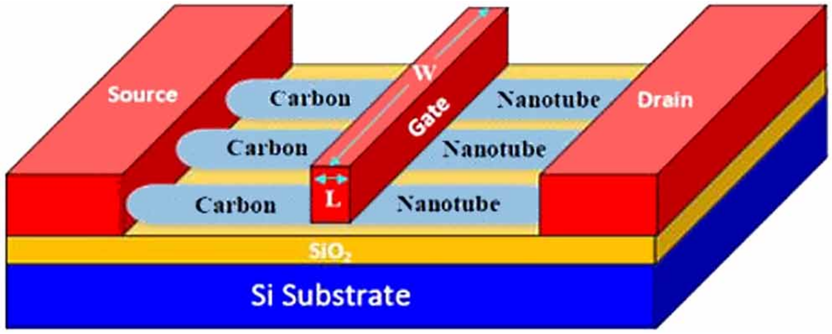


Figure 8.

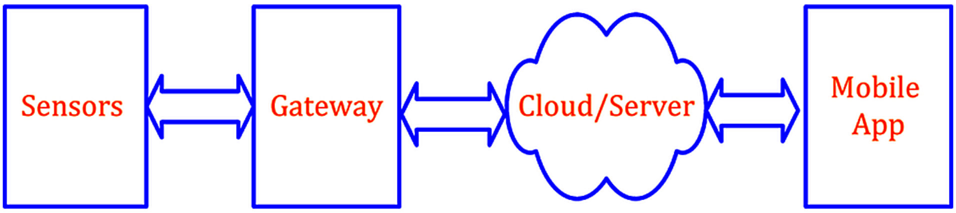
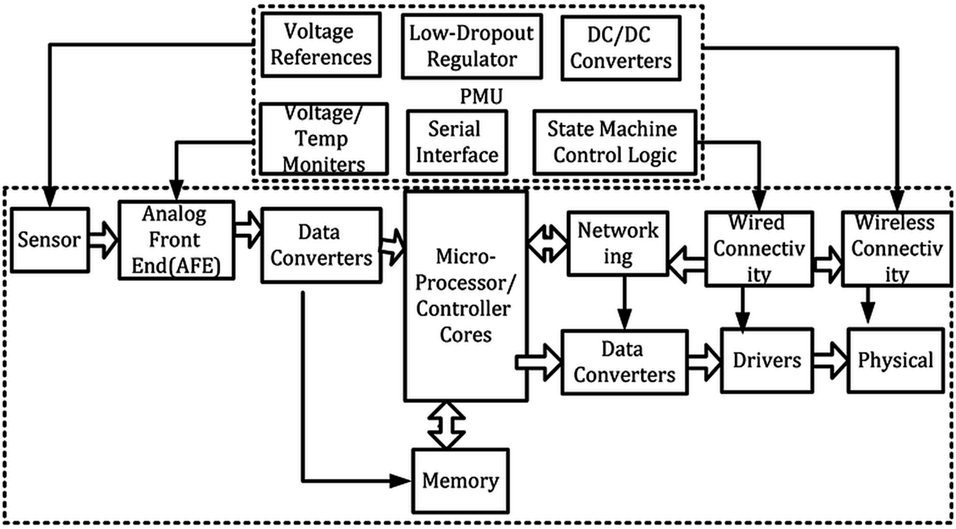


Figure 9.


Voltage References
Low-Dropout Regulator
DC/DC Converters
PMU
Voltage/ Temp Moniters
Serial Interface
State Machine Control Logic
Sensor
Analog Front End(AFE)
Data Converters
Micro-Processor/ Controller Cores
Network ing
Wired Connectiv ity
Wireless Connectiv ity
Data Converters
Drivers
Physical
Memory

Compilation of References

Pozar, D. M. (2011). Microwave Engineering. John Wiley & Sons.

Hlali, A., Houaneb, Z., & Zairi, H. (2019a). Tunable filter based on hybrid metal- graphene structures over an ultrawide terahertz band using an improved Wave Concept Iterative Process method. *International Journal for Light and Electron Optics*, *181*, 423–431. doi:10.1016/j.ijleo.2018.12.091

Hlali, A., Houaneb, Z., & Zairi, H. (2019b). Effective Modeling of Magnetized Graphene by the Wave Concept Iterative Process Method Using Boundary Conditions. *Progress In Electromagnetics Research C*, *89*, 121–132. doi:10.2528/PIERC18111514

Hlali, A., Houaneb, Z., & Zairi, H. (2018). Dual-Band Reconfigurable Graphene-Based Patch Antenna in Terahertz Band: Design, Analysis and Modeling Using WCIP Method. *Progress In Electromagnetics Research C*, *87*, 213–226. doi:10.2528/PIERC18080107

Tang, W. L., Zhang, H. Ch., Ma, H. F., Jiang, W. X., & Cui, T. J. (2019). Concept, Theory, Design, and Applications of Spoof Surface Plasmon Polaritons at Microwave Frequencies. *Advanced Optical Materials, 7*, 1–22.

Chen, H., Lu, W. B., Lui, Z. G., Zhang, J., & Huang, B. H. (2018). Efficient Manipulation of Spoof Surface Plasmon Polaritons Based on Rotated Complementary H-Shaped Resonator Metasurface. *IEEE Transactions on Antennas and Propagation*, *65*(12), 7383–7388. doi:10.1109/TAP.2017.2763175

Kianinejad, A., Chen, Z. N., & Qiu, Ch. W. (2015). Design and Modeling of Spoof Surface Plasmon Modes-Based Microwave Slow-Wave Transmission Line. *IEEE Transactions on Microwave Theory and Techniques*, *63*(6), 1817–1825. doi:10.1109/TMTT.2015.2422694

Kianinejad, A., Chen, Z. N., & Qiu, C.-W. (2018). Full Modeling, Loss Reduction, and Mutual Coupling Control of Spoof Surface Plasmon-Based Meander Slow Wave Transmission Lines. *IEEE Transactions on Microwave Theory and Techniques*, *66*(8), 3764–3772. doi:10.1109/TMTT.2018.2841857

Zhang, X., Zhang, H. Ch., Tang, W. X., Liu, J. F., Fang, Z., Wu, J. W., & Cui, J. W. (2017). Loss Analysis and Engineering of Spoof Surface Plasmons Based on Circuit Topology. *IEEE Antennas and Wireless Propagation Letters*, *16*, 3204–3207. doi:10.1109/LAWP.2017.2768551

Zhang, A. Q., Lu, W. B., Liu, Z. G., Chen, H., & Huang, B. H. (2018). Dynamically Tunable Substrate Integrated Waveguide Attenuator Using Graphene. *IEEE Transactions on Microwave Theory and Techniques*, *66*(6), 3081–3089. doi:10.1109/TMTT.2018.2809577

Zhang, A. Q., Liu, Z. G., Lu, W. B., & Chen, H. (2019a). Dynamically Tunable Attenuator on a Graphene-Based Microstrip Line. *IEEE Transactions on Microwave Theory and Techniques*, *67*(2), 746–753. doi:10.1109/TMTT.2018.2885761

Zhang, A. Q., Lu, W. B., Liu, Z. G., Wu, B., & Chen, H. (2019). Flexible and Dynamically Tunable Attenuator Based on Spoof Surface Plasmon Polaritons Waveguide Loaded With Graphene. *IEEE Transactions on Antennas and Propagation*, *67*(8), 5582–5589. doi:10.1109/TAP.2019.2911590

Zhang, A. Q., Liu, Z. G., Lu, W. B., & Chen, H. (2019b). Graphene-Based Dynamically Tunable Attenuator on a Coplanar Waveguide or a Slotline. *IEEE Transactions on Microwave Theory and Techniques*, *67*(1), 70–77. doi:10.1109/TMTT.2018.2875078

Aazam, M., & Huh, E. N. (2014, August). Fog computing and smart gateway based communication for cloud of things. In *2014 International Conference on Future Internet of Things and Cloud* (pp. 464-470). IEEE. 10.1109/FiCloud.2014.83

Abi Sen, A. A., & Yamin, M. (2020). Advantages of using fog in IoT applications. *International Journal of Information Technology*, 1-9.

Abraham, A., Pedregosa, F., Eickenberg, M., Gervais, P., Mueller, A., Kossaifi, J., Gramfort, A., Thirion, B., & Varoquaux, G. (2014). Machine learning for neuroimaging with scikit-learn. *Frontiers in Neuroinformatics*, *8*, 14. doi:10.3389/fninf.2014.00014 PMID:24600388

Adimulam, M. K., & Srinivas, M. B. (2017, November). Ultra-low power programmable wireless exg soc design for iot healthcare system. In *International Conference on Wireless Mobile Communication and Healthcare* (pp. 41-49). Springer.

Ahad, A., Tahir, M., & Yau, K. L. A. (2019). 5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 100747–100762. doi:10.1109/ACCESS.2019.2930628

Akeela, R., & Dezfouli, B. (2018). Software-defined radios: Architecture, state-of-the-art, and challenges. *Computer Communications*, *128*, 106–125. doi:10.1016/j.comcom.2018.07.012

Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5G networks for the Internet of Things: Communication technologies and challenges. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 3619–3647.

Al-Ali, A. R., & Al-Rousan, M. (2004). Java-based home automation system. *IEEE Transactions on Consumer Electronics*, *50*(2), 498–504. doi:10.1109/TCE.2004.1309414

Alavi, A., Tellambura, C., & Fair, I. (2005). PAPR reduction of OFDM signals using partial transmit sequence: An optimal approach using sphere decoding. *IEEE Communications Letters*, *9*(11), 982–984. doi:10.1109/LCOMM.2005.11014

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. doi:10.1109/COMST.2015.2444095

Al-Khafajiy, M., Webster, L., Baker, T., & Waraich, A. (2018, June). Towards fog driven IoT healthcare: challenges and framework of fog computing in healthcare. In *Proceedings of the 2nd international conference on future networks and distributed systems* (pp. 1-7). 10.1145/3231053.3231062

Aloysius, A., & Arockiam, L. (2012). Coupling complexity metric: A cognitive approach. *International Journal of Information Technology and Computer Science*, *4*(9), 29–35. doi:10.5815/ijitcs.2012.09.04

Al-Qaseemi, S. A., Almulhim, H. A., Almulhim, M. F., & Chaudhry, S. R. (2016, December). IoT architecture challenges and issues: Lack of standardization. In 2016 Future technologies conference (FTC) (pp. 731-738). IEEE.

Alzubi, J., Nayyar, A., & Kumar, A. (2018). Machine Learning from Theory to Algorithms: An Overview. *Journal of Physics: Conference Series*, *1142*(1), 012012. Advance online publication. doi:10.1088/1742-6596/1142/1/012012

Apache OpenNLP. (n.d.). Retrieved March 26, 2022, from https://opennlp.apache.org/

Armitage, S. (2006). Low-cost 2.4 GHz spectrum analyser. *Circuit Cellar*, *189*, 18–22.

Armstrong, J. (2002). Peak-to-average power reduction for OFDM by repeated clipping and frequency domain filtering. *Electronics Letters*, *38*(5), 246. doi:10.1049/el:20020175

Arne Holst. (2021, Oct 19). *Number of IoT connected devices worldwide 2019-2030*. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

ASIC design starts for 2022 by Key End Market Applications. (2022). Retrieved February 10, 2022 from https://semico.com/content/asic-design-starts-2022-key-end-market-applications

ASTM International. (2003). ASTM G48-03 Standard Test Methods for Pitting and Crevice Corrosion Resistance of Stainless Steels and Related Alloys by Use of Ferric Chlorde Solution. *ASTM G48-03*, 1-11.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787–2805. doi:10.1016/j.comnet.2010.05.010

Azarnia, G., Sharifi, A. A., & Emami, H. (2020). Compressive sensing based PAPR reduction in OFDM systems: Modified orthogonal matching pursuit approach. *ICT Express*, *6*(4), 368–371. doi:10.1016/j.icte.2020.07.004

Babu, S. M., Lakshmi, A. J., & Rao, B. T. (2015, April). A study on cloud based Internet of Things: CloudIoT. In 2015 global conference on communication technologies (GCCT) (pp. 60-65). IEEE.

Baccarani, G., Wordeman, M. R., & Dennard, R. H. (1984). Generalized scaling theory and its application to a 1/4 micrometer MOSFET design. *IEEE Transactions on Electron Devices*, *31*(4), 452–462.

Badr, H. M., Habib, M. A., Ben-Mansour, R., & Said, S. (2005). Numerical Investigation of Erosion Threshold Velocity in a Pipe With Sudden Contraction. *Computers & Fluids*, *34*(6), 721–742. doi:10.1016/j.compfluid.2004.05.010

Bahadori, A. (2015). *Essentials of Coating, Painting, and Lining for the Oil, Gas, and Petrochemical Industries*. Elsevier Inc.

Baier, T. C. (2007). A low budget vector network analyser for AF to UHF. *QEX*, 46–54.

Baier, T. C. (2009). A small, simple, USB-powered vector network analyser covering 1 kHz to 1.3 GHz. *QEX*, 32–36.

Baldoni, R. (2014). *Critical infrastructure protection: threats, attacks, and counter-measures*. Technical Report. Available online: http://www. dis. uniroma1. it/~ tenace….

Barnum, S. (2008). *Common attack pattern enumeration and classification (capec) schema description.* Http://Capec. Mitre. Org/Documents/Documentation/CAPEC_Schema_DescrIption_v1,3

Barnum, S. (2012). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX). *Mitre Corporation*, *11*, 1–22.

Basili, V. R., Briand, L. C., & Melo, W. L. (1996). A validation of object-oriented design metrics as quality indicators. *IEEE Transactions on Software Engineering*, *22*(10), 751–761. doi:10.1109/32.544352

Batta, M. (2020). Machine Learning Algorithms - A Review. *International Journal of Science and Research, 9*(1). doi:10.21275/ART20203995

Bäuml, R. W., Fischer, R. F. H., & Huber, J. B. (1996). Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping. *Electronics Letters*, *32*(22), 2056. doi:10.1049/el:19961384

Benini, L., & De Micheli, G. (2002). Networks on chips: A new SoC paradigm. *Computer, 35*(1), 70-78.

Bharathi, N., & Jayavel, K. (2021, December). Role of VLSI Design To Build Trusted And Secured IOT Devices-A Methodological Approach. In *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 473-479). IEEE.

Bhardwaj, R., Nambiar, A. R., & Dutta, D. (2017). A Study of Machine Learning in Healthcare. *Proceedings - International Computer Software and Applications Conference, 2*, 236–241. 10.1109/COMPSAC.2017.164

Bing, K., Fu, L., Zhuo, Y., & Yanlei, L. (2011, July). Design of an Internet of Things-based smart home system. In *2011 2nd International Conference on Intelligent Control and Information Processing* (Vol. 2, pp. 921-924). IEEE. 10.1109/ICICIP.2011.6008384

Biswas, A. R., & Giaffreda, R. (2014, March). IoT and cloud convergence: Opportunities and challenges. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 375-376). IEEE.

Blume, S. W. (2007). *Electrical Power Systems Basics: For the Nonelectrical Professional*. John Wiley & Sons. doi:10.1002/9780470185810

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16). 10.1145/2342509.2342513

Bor, M., Vidler, J. E., & Roedig, U. (2016). *LoRa for the Internet of Things*. Academic Press.

Borkar, S. (1999). Design challenges of technology scaling. *IEEE Micro*, *19*(4), 23–29.

Borsuk, G. M., & Coffey, T. (2003). Moore's Law: a department of defense perspective (No. 30). Center for Technology and National Security Policy, National Defense University.

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, *56*, 684–700. doi:10.1016/j.future.2015.09.021

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342–353. doi:10.1016/j.technovation.2014.02.001

Breiling, H., Muller-Weinfurtner, S. H., & Huber, J. B. (2001). SLM peak-power reduction without explicit side information. *IEEE Communications Letters*, *5*(6), 239–241. doi:10.1109/4234.929598

Briand, L. C., Daly, J. W., & Wüst, J. K. (1999). A unified framework for coupling measurement in object-oriented systems. *IEEE Transactions on Software Engineering*, *25*(1), 91–121. doi:10.1109/32.748920

Brito, J. M. C. (2018). Technological trends for 5G networks influence of E-Health and IoT applications. *International Journal of E-Health and Medical Communications*, *9*(1), 1–22. doi:10.4018/IJEHMC.2018010101

Bui, A., Johnson, F., & Wasko, C. (2019). The Relationship of Atmospheric Air Temperature and Dew Point Temperature to Extreme Rainfall. *Environmental Research Letters*, *14*(7), 1–8. doi:10.1088/1748-9326/ab2a26

Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2016). IoT-based big data storage systems in cloud computing: Perspectives and challenges. *IEEE Internet of Things Journal*, *4*(1), 75–87. doi:10.1109/JIOT.2016.2619369

Calhoun, B. H., & Wentzloff, D. D. (2015, August). Ultra-low power wireless SoCs enabling a batteryless IoT. In *Hot Chips Symposium* (pp. 1-45). Academic Press.

Canali, D., Bilge, L., & Balzarotti, D. (2014). On the effectiveness of risk prediction based on users browsing behavior. *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, 171–182. 10.1145/2590296.2590347

Candes, E. J., & Wakin, M. B. (2008). An Introduction To Compressive Sampling. *IEEE Signal Processing Magazine*, *25*(2), 21–30. doi:10.1109/MSP.2007.914731

Capretz, L. F., & Xu, J. (2008). An empirical validation of object-oriented design metrics for fault prediction. *Journal of Computational Science*, *4*(7), 571–577. doi:10.3844/jcssp.2008.571.577

Casesnoves, F., & Surzhenkov, A. (2017). A Mathematical Model For Abrasive Erosion Wear In Composite Fe-Based Matrix With WC-CO Reinforcement. *WIT Transactions on Engineering Sciences*, *116*, 99–111. doi:10.2495/MC170101

Castro. (2020). GPRS network prototype based on SDR and OpenBTS, as an IoT-lab Testbed. In *Seventh International Conference on Software Defined Systems (SDS)*. IEEE Publisher.

Castro, J., Kolp, M., & Mylopoulos, J. (2002). Towards requirements-driven information systems engineering: The Tropos project. *Information Systems*, *27*(6), 365–389. doi:10.1016/S0306-4379(02)00012-1

Chakravarthi, V. S. (2019). *A Practical Approach to VLSI System on Chip (SoC) Design: A Comprehensive Guide*. Springer Nature.

Chamola, V., Patra, S., Kumar, N., & Guizani, M. (2020). FPGA for 5G: Re-configurable hardware for next generation communication. *IEEE Wireless Communications*, *27*(3), 140–147. doi:10.1109/MWC.001.1900359

Charleonnan, A., Fufaung, T., Niyomwong, T., Chokchueypattanakit, W., Suwannawach, S., & Ninchawee, N. (2017). Predictive analytics for chronic kidney disease using machine learning techniques. *2016 Management and Innovation Technology International Conference, MITiCON 2016*, MIT80–MIT83. 10.1109/MITICON.2016.8025242

Chen, L., Zhou, X., Chen, F., Yang, L.-L., & Chen, R. (2021). Carrier phase ranging for indoor positioning with 5G NR signals. *IEEE Internet of Things Journal.*

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 Journal, 1*(4), 349-359.

Chen, G., Ansari, R., & Yao, Y. (2009). Improved peak windowing for PAPR reduction in OFDM. *IEEE Vehicular Technology Conference*, 4–8. 10.1109/VETECS.2009.5073593

Cheng, X., Zhang, C., Qian, Y., Aloqaily, M., & Xiao, Y. (2021). Editorial: Deep learning for 5G IoT systems. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3049–3051. doi:10.100713042-021-01382-w PMID:34306244

Chen, H., & Haimovich, A. M. (2003). Iterative estimation and cancellation of clipping noise for OFDM signals. *IEEE Communications Letters*, *7*(7), 305–307. doi:10.1109/LCOMM.2003.814720

Chen, J.-C., Chiu, M.-H., Yang, Y.-S., & Li, C.-P. (2011). A Suboptimal Tone Reservation Algorithm Based on Cross-Entropy Method for PAPR Reduction in OFDM Systems. *IEEE Transactions on Broadcasting*, *57*(3), 752–756. doi:10.1109/TBC.2011.2127590

Chen, J.-C., & Wen, C.-K. (2010). PAPR Reduction of OFDM Signals Using Cross-Entropy-Based Tone Injection Schemes. *IEEE Signal Processing Letters*, *17*(8), 727–730. doi:10.1109/LSP.2010.2051617

Chen, P. P.-S. (1976). The entity-relationship model—Toward a unified view of data. *ACM Transactions on Database Systems*, *1*(1), 9–36. doi:10.1145/320434.320440

Chen, X. Y., & Jin, Z. G. (2012). Research on key technology and applications for internet of things. *Physics Procedia*, *33*, 561–566. doi:10.1016/j.phpro.2012.05.104

Chettri, L., & Bera, R. (2019). A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal*, *7*(1), 16–32. doi:10.1109/JIOT.2019.2948888

Chhikara, A., Chhillar, R., & Khatri, S. (2011). Evaluating the impact of different types of inheritance on the object oriented software metrics. *International Journal of Enterprise Computing and Business Systems*, *1*(2), 1–7.

Chidamber, S. R., & Kemerer, C. F. (1994). A metrics suite for object oriented design. *IEEE Transactions on Software Engineering*, *20*(6), 476–493. doi:10.1109/32.295895

Chih-Tang, S. (1988). Evolution of the MOS transistor-from conception to VLSI. *Proceedings of the IEEE*, *76*(10), 1280–1326.

Choi, Y., Cardie, C., Riloff, E., & Patwardhan, S. (2005). Identifying sources of opinions with conditional random fields and extraction patterns. *Proceedings of human language technology conference and conference on empirical methods in natural language processing*, 355-362. 10.3115/1220575.1220620

Choudary, R. B. (2003). *Materials Science & Metallurgy* (1st ed.). Khanna Publishers.

Choudhary, G., & Jain, A. K. (2016, December). Internet of Things: A survey on architecture, technologies, protocols and challenges. In *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* (pp. 1-8). IEEE. 10.1109/ICRAIE.2016.7939537

Cicek, V. (2013). *Cathodic Protection: Industrial Solutions For Protecting Against Corrosion*. Scrivener Publishing LLC. doi:10.1002/9781118737880

Colwell, R. (2013, August). The chip design game at the end of Moore's law. In *2013 IEEE Hot Chips 25 Symposium (HCS)* (pp. 1-16). IEEE Computer Society.

Consortium, W. A. S. (2009). *Web application security consortium threat classification*. Author.

Cordero, C. J., Landicho, L. C. L., dela Cruz, J. C., & Garcia, R. G. (2017). Quantifying blood glucose level using S11 parameters. In *IEEE Region 10 Conference TENCON*. IEEE Publisher. doi:10.1109/TENCON.2017.8228091

Cord, O. (2001). *Genetic fuzzy systems: evolutionary tuning and learning of fuzzy knowledge bases* (Vol. 19). World Scientific. doi:10.1142/4177

Cordón, O. (2011). A historical review of evolutionary learning methods for Mamdani-type fuzzy rule-based systems: Designing interpretable genetic fuzzy systems. *International Journal of Approximate Reasoning*, *52*(6), 894–913. doi:10.1016/j.ijar.2011.03.004

Counsell, S., Mendes, E., & Swift, S. (2002). Comprehension of object-oriented software cohesion: The empirical quagmire. *Proceedings of the 10th International Workshop on Program Comprehension (IWPC)*, 33–42. 10.1109/WPC.2002.1021308

D'Ambros, M., Lanza, M., & Robbes, R. (2010). An extensive comparison of bug prediction approaches. *7th IEEE Working Conference on Mining Software Repositories (MSR)*, 31–41. 10.1109/MSR.2010.5463279

Dai, W., & Milenkovic, O. (2009). Subspace Pursuit for Compressive Sensing Signal Reconstruction. *IEEE Transactions on Information Theory*, *55*(5), 2230–2249. doi:10.1109/TIT.2009.2016006

Dalziell, E. P., & McManus, S. T. (2004). *Resilience, vulnerability, and adaptive capacity: Implications for system performance*. Academic Press.

Dang, T., Anghel, L., & Leveugle, R. (2006, September). Cntfet basics and simulation. In *International Conference on Design and Test of Integrated Systems in Nanoscale Technology, 2006. DTIS 2006.* (pp. 28-33). IEEE.

Das, R. K., Panda, M., & Dash, S. S. (2019). Smart agriculture system in India using internet of things. In *Soft computing in data analytics* (pp. 247–255). Springer. doi:10.1007/978-981-13-0514-6_25

De Campos, L. M., & Romero, A. E. (2009). Bayesian network models for hierarchical text classification from a thesaurus. *International Journal of Approximate Reasoning*, *50*(7), 932–944. doi:10.1016/j.ijar.2008.10.006

De Donno, M., Tange, K., & Dragoni, N. (2019). Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 150936–150948. doi:10.1109/ACCESS.2019.2947652

Depold, A., Erhardt, S., Weigel, R., & Lurz, F. (2021). A 10kHz to 6GHz low-cost vector network analyzer. *Advances in Radio Science*, *19*, 17–22. doi:10.5194/ars-19-17-2021

Devices, A. (2021). *RF, microwave, and millimeter wave products: selection guide 2021*. RF, Microwave, and Millimeter Wave Products.

Dietterich, T. G. (2000). Ensemble methods in machine learning. *International workshop on multiple classifier systems*, 1–15. 10.1007/3-540-45014-9_1

Dittmeier, C., & Casati, P. (2014). *Evaluating Internal Control Systems: A Comprehensive Assessment Model (CAM) for Enterprise Risk Management*. The Institute of Internal Auditors Research Foundation.

Do, K. H., & Roy, S. K. (1994). Corrosion of steel in tropical sea water. *British Corrosion Journal*, *29*(3), 233–236. doi:10.1179/000705994798267665

Donoho, D. L., Tsaig, Y., Drori, I., & Starck, J.-L. (2012). Sparse Solution of Underdetermined Systems of Linear Equations by Stagewise Orthogonal Matching Pursuit. *IEEE Transactions on Information Theory*, *58*(2), 1094–1121. doi:10.1109/TIT.2011.2173241

Doris, B., Ieong, M., Zhu, T., Zhang, Y., Steen, M., Natzle, W., . . . Haensch, W. (2003, December). Device design considerations for ultra-thin SOI MOSFETs. In *IEEE International Electron Devices Meeting 2003* (pp. 27-3). IEEE.

Doshi, J., Patel, T., & Kumar Bharti, S. (2019). Smart Farming using IoT, a solution for optimally monitoring farming conditions. *Procedia Computer Science*, *160*, 746–751. doi:10.1016/j.procs.2019.11.016

Dupont, J. N., Lippold, J. C., & Kiser, S. D. (2009). *Welding Metallurgy and Weldability of Nickel-Base Alloys*. John Wiley & Sons. doi:10.1002/9780470500262

Ebeling, C. E. (1997). *An Introduction To Reliability and Maintainability Engineering*. The McGraw-Hill Companies.

Ebert, C., Cain, J., Antoniol, G., Counsell, S., & Laplante, P. (2016). Cyclomatic complexity. *IEEE Software*, *33*(6), 27–29. doi:10.1109/MS.2016.147

Edeleanu, C. (1960). Corrosion Control By Anodic Protection. *Platinum Metals Review*, *4*(3), 86–91.

Edited by Boyer Howard E. (2020). *Ninth Printing). Atlas of Fatigue Curves*. ASM International.

El Emam, K., Melo, W., & Machado, J. C. (2001). The prediction of faulty classes using object-oriented design metrics. *Journal of Systems and Software*, *56*(1), 63–75.

Elfergani, H. A., & Abdalla, A. A. (2017). Effect of Chloride Concentration on the Corrosion Rate of Carbon Steel. In *2nd Libyan Conference On Chemistry and Its Application (LCCA)* (pp. 33-38). Benghazi: Libyan Conference on Chemistry and Its Application.

El-Samie, F., Al-kamali, F., Al-nahari, A., & Dessouky, M. (2013). *SC-FDMA for Mobile Communications*. CRC Press. doi:10.1201/b15157

Elsevier. (1991). Fundamentals of Fluid Dynamics. *International Geophysics, 47*, 7-83. doi:10.1016/S0074-6142(09)60056-5

Elsheakh, D. M., Ahmed, M. I., Elashry, G. M., Moghannem, S. M., Elsadek, H. A., Elmazny, W. N., Alieldin, N. H., & Abdallah, E. A. (2021). Rapid detection of coronavirus (Covid-19) using microwave immunosensor cavity resonator. *Sensors (Basel)*, *21*(21), 7021. doi:10.339021217021 PMID:34770328

Ergen, S. C. (2004). *ZigBee/IEEE 802.15. 4 Summary.* UC Berkeley.

Ertas, A. (2012). *Engineering Mechanics and Design Applications: Transdisciplinary Engineering Fundamentals*. Taylor & Francis Group, LLC.

EU FP7 Project CASAGRAS, (2009). *CASAGRAS Final Report: RFID and the Inclusive Model for the Internet of Things*. Author.

Evgeniou, T., & Pontil, M. (2001). Support vector machines: Theory and applications. Lecture Notes in Computer Science, 2049, 249–257. doi:10.1007/3-540-44673-7_12

Experian. (2015). *2015 second annual data breach industry forecast*. Author.

Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 156237–156271. doi:10.1109/ACCESS.2019.2949703

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *International Journal of Computers and Applications*, *113*(1), 1–7.

Fettweis, G. P. (2016, September). 5G and the future of IoT. In *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference* (pp. 21-24). IEEE.

Figueiredo, M., Nowak, R. D., & Wright, S. J. (2007). Gradient Projection for Sparse Reconstruction: Application to Compressed Sensing and Other Inverse Problems. *IEEE Journal of Selected Topics in Signal Processing*, *1*(4), 586–597. doi:10.1109/JSTSP.2007.910281

Fikri, D. N., Prajitno, P., & Wijaya, S. K. (2019). Development of microwave tomography system based on Arduino Nano and PocketVNA. In *2019 IEEE Conference on Antenna Measurements & Applications (CAMA)*. IEEE Publisher. 10.1109/CAMA47423.2019.8959618

Flandre, D., Colinge, J. P., Chen, J., De Ceuster, D., Eggermont, J. P., Ferreira, L., ... Silveira, F. (1999). Fully-depleted SOI CMOS technology for low-voltage low-power mixed digital/analog/microwave circuits. *Analog Integrated Circuits and Signal Processing*, *21*(3), 213–228.

Fortune Business Insights. (2021). *Internet of Things (IoT) Market Size, Share & COVID-19 Impact Analysis, By Component (Platform, Solution & Services), By End-Use Industry (BFSI, Retail, Government, Healthcare, Manufacturing, Agriculture, Sustainable Energy, Transportation, IT & Telecom, Others), and Regional Forecast, 2021-2028*. https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., Blackbird, J., Low, M. K., Mazurek, D., & McKinney, D. (2011). Symantec internet security threat report trends for 2010. *Volume XVI*.

Frank, D. J., Dennard, R. H., Nowak, E., Solomon, P. M., Taur, Y., & Wong, H. S. P. (2001). Device scaling limits of Si MOSFETs and their application dependencies. *Proceedings of the IEEE*, *89*(3), 259–288.

Frenzel, L. E. Jr. (2018). *Electronic Explained: Fundamentals for Engineers, Technicians, and Makers* (2nd ed.). Elsevier Inc.

Friha, O., Ferrag, M. A., Shu, L., Maglaras, L. A., & Wang, X. (2021). Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies. *IEEE CAA J. Autom. Sinica*, *8*(4), 718–752. doi:10.1109/JAS.2021.1003925

Gaikwad, P. P., Gabhane, J. P., & Golait, S. S. (2015, April). A survey based on Smart Homes system using Internet-of-Things. In *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)* (pp. 330-335). IEEE. 10.1109/ICCPEIC.2015.7259486

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, *30*(1), 28–38. doi:10.1109/MTS.2011.940293

Gannapathy, V. R., Tuani Ibrahim, A. F., Zakaria, Z., Othman, A. R., & Jalaudin, N. Q.Vigneswara Rao Gannapathy. (2014). A review on various types of software defined radios (SDRS) in radio communication. *International Journal of Research in Engineering and Technology*, *3*(12), 203–209. doi:10.15623/ijret.2014.0312026

Gavrila, C., Alexandru, M., Popescu, V., Sacchi, C., & Giusto, D. (2019). Satellite SDR gateway for M2M and IoT applications. In *IEEE Aerospace Conference*. IEEE Publisher. 10.1109/AERO.2019.8741705

Gershenfeld, N., & Marder, M. (1999). When Things Start to Think and the Nature of Matheinatical Modeling. *Physics Today*, *52*(10), 75. doi:10.1063/1.882867

Ghasem, N., & Henda, R. (2009). *Principles of Chemical Engineering Processes*. Taylor & Francis Group, LLC.

Glastone, S., & Mehra, V. (2011). Practical Fundamentals of Chemical Engineering (8th ed.). IDC Technologies.

Gokceli, S., Campo, P. P., Levanen, T., Yli-Kaakinen, J., Turunen, M., Allen, M., Riihonen, T., Palin, A., Renfors, M., & Valkama, M. (2020). SDR prototype for clipped and fast-convolution filtered OFDM for 5G New Radio uplink. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 89946–89963. doi:10.1109/ACCESS.2020.2993871

Gomez, C., Veras, J. C., Vidal, R., Casals, L., & Paradells, J. (2019). A sigfox energy consumption model. *Sensors (Basel)*, *19*(3), 681.

Goodpaster, K. E. (1991). Business ethics and stakeholder analysis. *Business Ethics Quarterly*, *1*(1), 53–73. doi:10.2307/3857592

GOST. (2009). *ISO/IEC 31010-2011 Risk management. Risk assessment methods*. ISO.

Goudos, S. K., Dallas, P. I., Chatziefthymiou, S., & Kyriazakos, S. (2017). A survey of IoT key enabling and future technologies: 5G, mobile IoT, sematic web and applications. *Wireless Personal Communications*, *97*(2), 1645–1675.

Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). *Cyber-Physical Systems and Internet of Things, Special Publication (NIST SP)*. National Institute of Standards and Technology. [online], doi:10.6028/NIST.SP.1900-202

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectureal elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Guinard, D., Trifa, V., Mattern, F., & Wilde, E. (2011). From the internet of things to the web of things: Resource-oriented architecture and best practices. In *Architecting the Internet of things* (pp. 97–129). Springer. doi:10.1007/978-3-642-19157-2_5

Gupta, A., & Jha, R. K. (2015). A Survey of 5G Network: Architecture and Emerging Technologies. *IEEE Access: Practical Innovations, Open Solutions*, *3*, 1206–1232. doi:10.1109/ACCESS.2015.2461602

Haanappel, V. A., & Stroosnijder, M. F. (2001). Influence of Mechanical Deformation on the Corrosion Behavior of AISI 304 Stainless Steel Obtained from Cooking Utensils. *Corrosion*, *57*(6), 557–565. doi:10.5006/1.3290382

HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129. doi:10.1016/j.iot.2019.100129

Han, S. H., Cioffi, J. M., & Lee, J. H. (2006). Tone injection with hexagonal constellation for peak-to-average power ratio reduction in OFDM. *IEEE Communications Letters*, *10*(9), 646–648. doi:10.1109/LCOMM.2006.1714532

Han, S. H., & Lee, J. H. (2004). Modified Selected Mapping Technique for PAPR Reduction of Coded OFDM Signal. *IEEE Transactions on Broadcasting*, *50*(3), 335–341. doi:10.1109/TBC.2004.834200

Han, S. H., & Lee, J. H. (2004). PAPR reduction of OFDM signals using a reduced complexity PTS technique. *IEEE Signal Processing Letters*, *11*(11), 887–890. doi:10.1109/LSP.2004.833490

Han, S. H., & Lee, J. H. (2005). An overview of peak-to-average power ratio reduction techniques for multicarrier transmission. *IEEE Wireless Communications*, *12*(2), 56–65. doi:10.1109/MWC.2005.1421929

Haron, N. Z., & Hamdioui, S. (2008, December). Why is CMOS scaling coming to an END? In *2008 3rd International Design and Test Workshop* (pp. 98-103). IEEE.

HarveyI. (2007). *Introduction To Managing Risk.* Academic Press.

Hegedűs, P. (2019). Towards analyzing the complexity landscape of solidity based ethereum smart contracts. *Technologies*, *7*(1), 6.

He, J., & Yan, Z. (2013). Improving convergence rate of active constellation extension algorithm for PAPR reduction in OFDM. *2013 IEEE International Conference on Information and Automation (ICIA)*, 280–284. 10.1109/ICInfA.2013.6720310

Henze, A., Tempone, N., Monasterios, G., & Silva, H. (2014). Incomplete 2-port vector network analyzer calibration methods. In *IEEE Biennial Congress of Argentina (ARGENCON)*. IEEE Publisher. 10.1109/ARGENCON.2014.6868593

Hipple, J. (2017). *Chemical Engineering for Non-Chemical Engineers*. American Institue of Chemical Engineers. doi:10.1002/9781119369196

Huang, X., & Lu, J. (n.d.). Companding transform for the reduction of peak-to-average power ratio of OFDM signals. *IEEE VTS 53rd Vehicular Technology Conference, Spring 2001. Proceedings, 2*, 835–839. 10.1109/VETECS.2001.944496

Huang, X., Lu, J., Zheng, J., Chuang, J., & Gu, J. (2001). Reduction of peak-to-average power ratio of OFDM signals with companding transform. *Electronics Letters*, *37*(8), 506. doi:10.1049/el:20010345

Hutchings, I. (1992). Abrasive and Erosive Wear of Metal-Matrix Composites. In *2nd European Conference on Advanced Materials and Processes*. London: Institute of Materials.

International Technology Roadmap for Semiconductors. (2011). Retrieved December 12, 2021, from http://www.itrs.net/

International Telecommunication Union. (2009). *Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)*. Report ITU-R SM.2152.

Intille, S. S. (2002). Designing a home of the future. *IEEE Pervasive Computing*, *1*(2), 76–82. doi:10.1109/MPRV.2002.1012340

Isaac, R. D. (1998, October). Reaching the limits of CMOS technology. In *IEEE 7th Topical Meeting on Electrical Performance of Electronic Packaging* (p. 3). IEEE.

Ishtiaq, A., Khan, M. U., Ali, S. Z., Habib, K., Samer, S., & Hafeez, E. (2021, August). A Review of System on Chip (SOC) Applications in Internet of Things (IOT) and Medical. In *ICAME21, International Conference on Advances in Mechanical Engineering* (pp. 1-10). Academic Press.

Islam, A. (2015, June). Technology scaling and its side effects. In *2015 19th International Symposium on VLSI Design and Test (VDAT)* (pp. 1-1). IEEE Computer Society.

Islam, M. M., Rahaman, A., & Islam, M. R. (2020). Development of Smart Healthcare Monitoring System in IoT Environment. *SN Computer Science*, *1*(3), 185. Advance online publication. doi:10.100742979-020-00195-y PMID:33063046

Jahromi, A. H., & Taheri, M. (2017). A non-parametric mixture of gaussian naive bayes classifiers based on local independent features. *2017 Artificial Intelligence and Signal Processing Conference (AISP)*, 209–212. 10.1109/AISP.2017.8324083

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5), e10059. doi:10.2196/10059 PMID:29807882

Javaid, N., Sher, A., Nasir, H., & Guizani, N. (2018). Intelligence in IoT-based 5G networks: Opportunities and challenges. *IEEE Communications Magazine*, *56*(10), 94–100. doi:10.1109/MCOM.2018.1800036

Jeon, H.-B., No, J.-S., & Shin, D.-J. (2012). A New PAPR Reduction Scheme Using Efficient Peak Cancellation for OFDM Systems. *IEEE Transactions on Broadcasting*, *58*(4), 619–628. doi:10.1109/TBC.2012.2211432

Jiang, T., & Wu, Y. (2008). An overview: Peak-to-average power ratio reduction techniques for OFDM signals. *Broadcasting*. *IEEE Transactions On*, *54*(2), 257–268. doi:10.1109/TBC.2008.915770

Jie, Y., Pei, J. Y., Jun, L., Yun, G., & Wei, X. (2013, June). Smart home system based on iot technologies. In *2013 International conference on computational and information sciences* (pp. 1789-1791). IEEE. 10.1109/ICCIS.2013.468

Jones, D. A. (1996). *Principles and Prevention of Corrosion* (2nd ed.). Prentice-Hall, Inc.

Jung, M., Hajdarevic, E., Kastner, W., & Jara, A. (2014, March). Short paper: A scripting-free control logic editor for the Internet of Things. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 193-194). IEEE.

Kandil, A., & El-Deeb, H. (2016, January). Exploration of application migration to cloud environment. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 109-114). IEEE. doi:10.1109/CONFLUENCE.2016.7508097

Kang, B. M., Ryu, H.-G., & Ryu, S. B. (2007). A PAPR Reduction Method using New ACE (Active Constellation Extension) with Higher Level Constellation. *2007 IEEE International Conference on Signal Processing and Communications*, 724–727. 10.1109/ICSPC.2007.4728421

Kassab, W. A., & Darabkh, K. A. (2020). A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, *163*, 102663. doi:10.1016/j.jnca.2020.102663

Kataria, S., & Beniwal, P. (2016). FinFET Technology: A Review Paper. *International Journal of Technical Research*, *5*(2).

Kececi, E. F. (2019). *Mechatronic Components: Roadmap to Design*. Elsevier Inc.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *2012 10th international conference on frontiers of information technology* (pp. 257-260). IEEE. 10.1109/FIT.2012.53

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411.

Kidd, C. D., Orr, R., Abowd, G. D., Atkeson, C. G., Essa, I. A., MacIntyre, B., ... Newstetter, W. (1999, October). The aware home: A living laboratory for ubiquitous computing research. In *International workshop on cooperative buildings* (pp. 191-198). Springer. 10.1007/10705432_17

Kilchytska, V., Andrieu, F., Faynot, O., & Flandre, D. (2011, March). High-temperature perspectives of UTB SOI MOSFETs. In *Ulis 2011 Ultimate Integration on Silicon* (pp. 1–4). IEEE.

Kim, K.-D., & Kumar, P. R. (2013). An overview and some challenges in cyber-physical systems. *Journal of the Indian Institute of Science*, *93*(3), 341–352.

Kitchenham, B. (2010). What's up with software metrics? –A preliminary mapping study. *Journal of Systems and Software*, *83*(1), 37–51. doi:10.1016/j.jss.2009.06.041

Knud Lasse Lueth. (2018, February 22). *The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects*. https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/

Kosa, E., & Goksenli, A. (2017). Influence of Material Hardness and Particle Velocity On Erosive Wear Rate. *Jixie Gongcheng Xuebao*, *47*, 8–14.

Kotecki, D. J., & Lippold, J. C. (2005). *Welding Metallurgy and Weldability of Stainless Steels*. John Wiley & Sons Inc.

Ko, U. (2016, April). Ultra-low power SoC for wearable & IoT. In *2016 International Symposium on VLSI Technology, Systems and Application (VLSI-TSA)* (pp. 1-1). IEEE.

Kraijak, S., & Tuwanut, P. (2015, September). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. In *11th international conference on wireless communications, networking and mobile computing (WiCOM 2015)* (pp. 1-6). IET. 10.1049/cp.2015.0714

Krok, M., & Gwarek, W. (2006). A low-cost PC controlled system for measurement of vector reflection coefficient in ISM band. In *International Conference on Microwaves, Radar & Wireless Communications*. IEEE Publisher. 10.1109/MIKON.2006.4345099

Krongold, B. S., & Jones, D. L. (2003). PAR reduction in OFDM via active constellation extension. *IEEE Transactions on Broadcasting*, *49*(3), 258–268. doi:10.1109/TBC.2003.817088

Krongold, B. S., & Jones, D. L. (2004). An Active-Set Approach for OFDM PAR Reduction via Tone Reservation. *IEEE Transactions on Signal Processing*, *52*(2), 495–509. doi:10.1109/TSP.2003.821110

Kullarni, V. Y., & Sinha, P. K. (2013). Random Forest Classifier: A Survey and Future Research Directions. *International Journal of Advanced Computing*, *36*(1), 1144–1156.

Kumar, R. P., & Smys, S. (2018, January). A novel report on architecture, protocols and applications in Internet of Things (IoT). In *2018 2nd International Conference on Inventive Systems and control (ICISC)* (pp. 1156-1161). IEEE.

Kumar, A., Dhanagopal, R., Albreem, M. A., & Le, D. N. (2021). A comprehensive study on the role of advanced technologies in 5G based smart hospital. *Alexandria Engineering Journal*, *60*(6), 5527–5536. doi:10.1016/j.aej.2021.04.016

Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. *Procedia Computer Science*, *132*, 109–117. doi:10.1016/j.procs.2018.05.170

Kumar, P. M., & Gandhi, U. D. (2018). A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. *Computers & Electrical Engineering*, *65*, 222–235. doi:10.1016/j.compeleceng.2017.09.001

Kuyoro, S., Osisanwo, F., & Akinsowon, O. (2015, March). Internet of things (IoT): an overview. In *Proc. of the 3rd International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM)* (pp. 23-24). Academic Press.

Lalonde Levesque, F., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013). A clinical study of risk factors related to malware infections. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 97–108. 10.1145/2508859.2516747

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440.

Lee, J. W., Kim, H. K., Oh, J. H., Yang, J. W., Lee, W. C., Kim, J. S., ... Koh, Y. H. (1998, October). A new SOI MOSFET for low power applications. In *1998 IEEE International SOI Conference Proceedings (Cat No. 98CH36199)* (pp. 65-66). IEEE.

Lee, S. K., Bae, M., & Kim, H. (2017). Future of IoT networks: A survey. *Applied Sciences (Basel, Switzerland)*, *7*(10), 1072. doi:10.3390/app7101072

Lee, Y.-L., You, Y.-H., Jeon, W.-G., Paik, J.-H., & Song, H.-K. (2003). Peak-to-average power ratio in MIMO-OFDM systems using selective mapping. *IEEE Communications Letters*, *7*(12), 575–577. doi:10.1109/LCOMM.2003.821329

Levy, A. V. (1995). *Solid Particle Erosion and Erosion-Corrosion of Materials*. ASM International.

Levy, A. V., & Chik, P. (1983). The Effects of Erodent Composition and Shape on the Erosion of Steel. *Wear*, *89*(2), 151–162. doi:10.1016/0043-1648(83)90240-5

Lexical Variant Generation (LVG). (n.d.). Retrieved March 26, 2022, from https://www.nlm.nih.gov/research/umls/new_users/online_learning/LEX_004.html

Li, C. P., Wang, S. H., & Wang, C. L. (2010). Novel low-complexity SLM schemes for PAPR reduction in OFDM systems. *IEEE Transactions on Signal Processing*, *58*(5), 2916–2921. doi:10.1109/TSP.2010.2043142

Li, H., Jiang, T., & Zhou, Y. (2011). An Improved Tone Reservation Scheme With Fast Convergence for PAPR Reduction in OFDM Systems. *IEEE Transactions on Broadcasting*, *57*(4), 902–906. doi:10.1109/TBC.2011.2169622

Lim, D.-W., Noh, H.-S., Jeon, H.-B., No, J.-S., & Shin, D.-J. (2009). Multi-Stage TR Scheme for PAPR Reduction in OFDM Signals. *IEEE Transactions on Broadcasting*, *55*(2), 300–304. doi:10.1109/TBC.2009.2013988

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 Journal*, *4*(5), 1125–1142. doi:10.1109/JIOT.2017.2683200

Lippold, J. C. (2015). *Welding Metallurgy and Weldability*. John Wiley & Sons, Inc. doi:10.1002/9781118960332

Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, *10*, 1–9.

Liu, T. J. K. (2012). Introduction to multi-gate MOSFETs. *6th Annual SOI Fundamentals Class, 3*.

Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M., & Liu, M. (2015). Cloudy with a chance of breach: Forecasting cyber security incidents. *24th USENIX Security Symposium (USENIX Security 15)*, 1009–1024.

Liu, E., & Temlyakov, V. N. (2012). The Orthogonal Super Greedy Algorithm and Applications in Compressed Sensing. *IEEE Transactions on Information Theory*, *58*(4), 2040–2047. doi:10.1109/TIT.2011.2177632

Liu, T. K. (2012, June). FinFET history, fundamentals and future. In *Proceedings of the Symposium on VLSI Technology Short Course*. University of California

Liu, Z., Qian, P., Wang, X., Zhuang, Y., Qiu, L., & Wang, X. (2021). Combining graph neural networks with expert knowledge for smart contract vulnerability detection. *IEEE Transactions on Knowledge and Data Engineering*, 1. doi:10.1109/TKDE.2021.3095196

Li, W., & Henry, S. (1993). Object-oriented metrics that predict maintainability. *Journal of Systems and Software*, *23*(2), 111–122. doi:10.1016/0164-1212(93)90077-B

Li, X., & Cimini, L. J. (1998). Effects of clipping and filtering on the performance of OFDM. *IEEE Communications Letters*, *2*(5), 131–133. doi:10.1109/4234.673657

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*.

Li, Y., & Wu, H. (2012). A Clustering Method Based on K-Means Algorithm. *Physics Procedia*, *25*, 1104–1109. doi:10.1016/j.phpro.2012.03.206

Lloret, J., Parra, L., Taha, M., & Tomás, J. (2017). An architecture and protocol for smart continuous eHealth monitoring using 5G. *Computer Networks*, *129*, 340–351. doi:10.1016/j.comnet.2017.05.018

Mack, C. (2015). The multiple lives of Moore's law. *IEEE Spectrum*, *52*(4), 31–31.

Mackensen, E., Lai, M., & Wendt, T. M. (2012, October). Bluetooth Low Energy (BLE) based wireless sensors. In SENSORS, 2012 IEEE (pp. 1-4). IEEE.

Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(05), 164.

Ma, H. D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer Science and Technology*, *26*(6), 919–924. doi:10.100711390-011-1189-5

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336-341). IEEE.

Majumber, S. (2018). Energy detection spectrum sensing on RTL-SDR based IoT platform. In *Conference on Information and Communication Technology*. IEEE Publisher.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *Unlocking the potential of the Internet of Things*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Marinho, D., Arruela, R., Varum, T., & Matos, J. N. (2020). Software-defined radio beamforming system for 5G/radar applications. *Applied Sciences (Basel, Switzerland)*, *10*(20), 7187. doi:10.3390/app10207187

Markov, I. L. (2014). Limits on fundamental limits to computation. *Nature*, *512*(7513), 147–154.

Markowski, A. S., & Mannan, M. S. (2009). Fuzzy logic for piping risk assessment (pfLOPA). *Journal of Loss Prevention in the Process Industries*, *22*(6), 921–927. doi:10.1016/j.jlp.2009.06.011

Martin, R. A. (2007). *Common weakness enumeration*. Mitre Corporation.

Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, *28*, 68–90. doi:10.1016/j.adhoc.2014.12.006

Ma, Y., Zeng, Y., & Sun, S. (2018). A software defined radio based multi-function radar for IoT applications. In *24th Asia-Pacific Conference on Communications (APCC)*. IEEE Publisher. 10.1109/APCC.2018.8633541

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. *African Journal of Information and Communication*, *23*(23), 1–26. doi:10.23962/10539/27535

McCabe, T. J. (1976). A complexity measure. *IEEE Transactions on Software Engineering*, *SE-2*(4), 308–320. doi:10.1109/TSE.1976.233837

McCallum, A. (2003). Efficiently inducing features of conditional random fields. *UAI'03: Proceedings of the Nineteenth Conference on Uncertainty in Artificial Intelligence*, 403–410.

McDermott, T. & Ireland, K. (2004). A low-cost 100 MHz vector network analyzer with USB interface. *QEX*, 3–14.

Meindl, J. D. (1983, December). Theoretical, practical and analogical limits in ULSI. In *1983 International Electron Devices Meeting* (pp. 8-13). IEEE.

Mitola, J. (1993). Software radios: Survey, critical evaluation and future directions. *IEEE Aerospace and Electronic Systems Magazine*, *8*(4), 25–36. doi:10.1109/62.210638

Mobin, M., & Shabnam, H. (2011). Corrosion Behavior of Mild Steel and SS 304L in Presence of Dissolved Nickel Under Aerated and DeAerated Conditions. *Materials Research*, *14*(4), 524–531. doi:10.1590/S1516-14392011005000076

Mohamed, M. A., Knoerzer, K., Mansour, M. P., Trujillo, F. J., Juliano, P., & Shrestha, P. (2020). Improved canola oil expeller extraction using a pilot-scale continuous flow microwave system for pre-treatment of seeds and flaked seeds. *Journal of Food Engineering*, *284*, 110053. doi:10.1016/j.jfoodeng.2020.110053

Moore, G. E. (1975, December). Progress in digital integrated electronics. In Electron devices meeting (Vol. 21, pp. 11-13). Academic Press.

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics (Basel)*, *38*(8).

Muangprathub, J., Boonnam, N., Kajornkasirat, S., Lekbangpong, N., Wanichsombat, A., & Nillaor, P. (2019). IoT and agriculture data analysis for smart farm. *Computers and Electronics in Agriculture*, *156*, 467–474. doi:10.1016/j.compag.2018.12.011

Müller, S. H., & Huber, J. B. (1997). OFDM with reduced peak-to-average power ratio by optimum combination of partial transmit sequences. *Electronics Letters*, *33*(5), 368. doi:10.1049/el:19970266

Mustafa, A., & Rahimi Azghadi, M. (2021). Automated machine learning for healthcare and clinical notes analysis. *Computers*, *10*(2), 1–31. doi:10.3390/computers10020024

Nair, R. (2002). Effect of increasing chip density on the evolution of computer architectures. *IBM Journal of Research and Development, 46*(2.3), 223-234.

Najm, I. A., Hamoud, A. K., Lloret, J., & Bosch, I. (2019). Machine learning prediction approach to enhance congestion control in 5G IoT environment. *Electronics (Switzerland)*, *8*(6), 607. Advance online publication. doi:10.3390/electronics8060607

Narayanan, R., Kumar, S., & Murthy, S. R. (2020). Cross technology distributed MIMO for low power IoT. *IEEE Transactions on Mobile Computing*.

Nditiru, S. (2021). SDRs as a reference and common clock source for GNSS timing apps. *Microwaves & RF*, 20–24.

Needell, D., & Tropp, J. A. (2009). CoSaMP: Iterative signal recovery from incomplete and inaccurate samples. *Applied and Computational Harmonic Analysis*, *26*(3), 301–321. doi:10.1016/j.acha.2008.07.002

Needell, D., & Vershynin, R. (2009). Uniform Uncertainty Principle and Signal Recovery via Regularized Orthogonal Matching Pursuit. *Foundations of Computational Mathematics*, *9*(3), 317–334. doi:10.100710208-008-9031-3

Nikonov, D. E., & Young, I. A. (2013). Overview of beyond-CMOS devices and a uniform methodology for their benchmarking. *Proceedings of the IEEE*, *101*(12), 2498–2533.

Nolan, S. M. (2018). Power Management for Internet of Things (IoT) System on a Chip (SoC). *Development.*

Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, *133*, 97–108.

Nowak, E. J. (2002). Maintaining the benefits of CMOS scaling when scaling bogs down. *IBM Journal of Research and Development, 46*(2.3), 169-180.

O'Neill, R., & Lopes, L. B. (n.d.). Envelope variations and spectral splatter in clipped multicarrier signals. *Proceedings of 6th International Symposium on Personal, Indoor and Mobile Radio Communications*, *1*, 71–75. 10.1109/PIMRC.1995.476406

Obi, E. R. (2008). *Corrosion Behaviour of Fly Ash-Reinforced Aluminum-Magnesium Alloy A535 Composites.* University of Saskatchewan, Mechanical Engineering. Retrieved from https://harvest.usask.ca/handle/10388/etd-09222008-235440

Ochiai, H., & Imai, H. (n.d.). On clipping for peak power reduction of OFDM signals. *Globecom '00 - IEEE. Global Telecommunications Conference. Conference Record, 2*, 731–735. 10.1109/GLOCOM.2000.891236

Ochiai, H., & Imai, H. (2002). Performance analysis of deliberately clipped OFDM signals. *IEEE Transactions on Communications*, *50*(1), 89–101. doi:10.1109/26.975762

Okonkwo, P. C. (2014). Erosion-Corrosion in Oil and Gas Industry: A Review. *International Journal Of Metallurgical & Material*, *4*(3), 7–28.

Oliva, G. A., & Gerosa, M. A. (2011). On the interplay between structural and logical dependencies in open-source software. *25th Brazilian Symposium on Software Engineering (SBES)*, 144–153. 10.1109/SBES.2011.39

Omoniwa, B., Hussain, R., Javed, M. A., Bouk, S. H., & Malik, S. A. (2018). Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. *IEEE Internet of Things Journal*, *6*(3), 4118–4149. doi:10.1109/JIOT.2018.2875544

Onasanya, A., & Elshakankiri, M. (2019). Smart integrated IoT healthcare system for cancer care. *Wireless Networks*, 1–16.

Oyj, N. (2016). *LTE evolution for IoT connectivity.* Nokia Corporation White Paper.

Painuly, S., Kohli, P., Matta, P., & Sharma, S. (2020, December). Advance applications and future challenges of 5G IoT. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 1381-1384). IEEE.

Pal, M. (2005). Random forest classifier for remote sensing classification. *International Journal of Remote Sensing*, *26*(1), 217–222. doi:10.1080/01431160412331269698

Pal, R. S., Sharma, S., & Dasgupta, S. (2017, March). Recent trend of FinFET devices and its challenges: A review. In *2017 Conference on Emerging Devices and Smart Systems (ICEDSS)* (pp. 150-154). IEEE.

Park, Y. T., Kuk, S. H., Kang, I. H., & Kim, H. G. (2017). Overcoming IoT language barriers using smartphone SDRs. *IEEE Transactions on Mobile Computing*, *16*(3), 816–828. doi:10.1109/TMC.2016.2570749

Parthasarathy, P., & Vivekanandan, S. (2020). A typical IoT architecture-based regular monitoring of arthritis disease using time wrapping algorithm. *International Journal of Computers and Applications*, *42*(3), 222–232. doi:10.1080/1206212X.2018.1457471

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., & Dubourg, V. (2011). Scikit-learn: Machine learning in python. *Journal of Machine Learning Research, 12*, 2825–2830.

Peña-López, I. (2005). *ITU Internet report 2005: the internet of things*. https://www.itu.int/osg/spu/publications/internetofthings/

Phillips, D. H. (2016). *Welding Engineering: An Introduction*. John Wiley & Sons Ltd. doi:10.1002/9781119191407

Pourbaix, M. (1974). *Atlas of Electrochemical Equilibria in Aqueous Solutions*. National Association of Corrosion Engineers.

Prabhu, R. S., & Grayver, E. (2009). Active constellation modification techniques for OFDM PAR reduction. *2009 IEEE Aerospace Conference*, 1–8. 10.1109/AERO.2009.4839406

Pradhan, K., & Chawla, P. (2020). Medical Internet of things using machine learning algorithms for lung cancer detection. *Journal of Management Analytics*, *7*(4), 591–623. doi:10.1080/23270012.2020.1811789

Pratama, B. Y., & Sarno, R. (2015). Personality classification based on twitter text using naive bayes, knn and svm. *2015 International Conference on Data and Software Engineering (ICoDSE)*, 170–174. 10.1109/ICODSE.2015.7436992

Pratt, T. G., Jones, N., Smee, L., & Torrey, M. (2006). OFDM Link Performance With Companding for PAPR Reduction in the Presence of Non-Linear Amplification. *IEEE Transactions on Broadcasting*, *52*(2), 261–267. doi:10.1109/TBC.2006.875613

Qiwei, Z., Faiz Zainuddin, M., Fahad Ahmad, A., Obays, S. J., & Abbas, Z., Qiwei, Z., Zainuddin, M. F., & Ahmad, A. F. (2019). Development of an Affordable Soil Moisture Sensor System with Mini-VNA Tiny and Smartphone. *Pertanika Journal of Science & Technology*, *27*(3), 1121–1129.

Radjenović, D., Heričko, M., Torkar, R., & Živkovič, A. (2013). Software fault prediction metrics: A systematic literature review. *Information and Software Technology*, *55*(8), 1397–1418. doi:10.1016/j.infsof.2013.02.009

Rahmatallah, Y., & Mohan, S. (2013). Peak-to-average power ratio reduction in ofdm systems: A survey and taxonomy. *IEEE Communications Surveys and Tutorials*, *15*(4), 1567–1592. doi:10.1109/SURV.2013.021313.00164

Rauf, S. B. (2014). *Electrical Engineeering for Non-Electrical Engineers*. The Fairmont Press, Inc.

Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences*, *30*(3), 291–319. doi:10.1016/j.jksuci.2016.10.003

Reite, B. (2019). PocketVNA review. *Radio Guide*, *27*(5), 14.

Revie, R. W., & Uhlig, H. H. (2008). *Corrosion and Corrosion Control: An Introduction to Corrosion Science and Engineering*. Wiley-InterScience. doi:10.1002/9780470277270

Rghioui, A., Lloret, J., Sendra, S., & Oumnad, A. (2020). A Smart Architecture for Diabetic Patient Monitoring Using Machine Learning Algorithms. *Health Care*, *8*(3), 348. doi:10.3390/healthcare8030348 PMID:32961757

Rohde & Schwarz. (2004a). Software defined radios – overview and hardware. *New from Rohde & Schwarz*, *182*, 58–61.

Rohde & Schwarz. (2004b). Software defined radios – software aspects and the future. *New from Rohde & Schwarz*, *183*, 52–55.

Rytting, D. (2001). VNA error models and calibration methods. In *Proc. ARFTG/NIST Short Course on RF Measurements for a Wireless World*. IEEE Publisher.

Saeedi, H., Sharif, M., & Marvasti, F. (2002). Clipping noise cancellation in OFDM systems using oversampled signal reconstruction. *IEEE Communications Letters*, *6*(2), 73–75. doi:10.1109/4234.984699

Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. *International Journal of Computer Networks*, *5*(1), 1–17.

Salas, P. (2011). Array Solutions VNA 2180 vector network analyser. *QST*, 57–59.

Salas, P. (2020). NanoVNA vector network analyser. *QST*, 39–43.

Santos-Luna, E. (2019). A spectrum analyser based on a low-cost hardware-software integration. In *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE Publisher.

Savova, G. K., Masanz, J. J., Ogren, P. V., Zheng, J., Sohn, S., Kipper-Schuler, K. C., & Chute, C. G. (2010). Mayo clinical Text Analysis and Knowledge Extraction System (cTAKES): Architecture, component evaluation and applications. *Journal of the American Medical Informatics Association: JAMIA*, *17*(5), 507–513. doi:10.1136/jamia.2009.001560 PMID:20819853

Schweitzer, P. A. (2006). *Paint and Coatings: Applications and Corrosion Resistance*. Taylor & Francis Group, LLC.

Sedriks, J. A. (1996). *Corrosion of Stainless Steels*. John Wiley & Sons, Inc.

Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: A systematic review. *SN Applied Sciences*, *2*(1), 1–8. doi:10.100742452-019-1925-y

Sepranos, D., & Wolf, M. (2019). Challenges and Opportunities in VLSI IoT Devices and Systems. *IEEE Design & Test*, *36*(4), 24–30.

Serozhenko, M. (2017, Jun 15). *Brief history of the internet of things*. https://medium.com/mqtt-buddy/brief-history-of-the-internet-of-things-f00043ae17b5

Sethi, P., & Sarangi, S. R. (2017). Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*, 2017. doi:10.1155/2017/9324035

Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 23022–23040. doi:10.1109/ACCESS.2020.2970118

Shalf, J. (2020). The future of computing beyond Moore's law. *Philosophical Transactions of the Royal Society A*, *378*(2166), 20190061.

Shehadeh, M., Anany, M., Saqr, K. M., & Hassan, I. (2014). Experimental Investigatio of Erosion-Corrosion Phenomena in a Steel Fitting Due to Plain and Slurry Seawater Flow. *International Journal of Mechanical and Materials Engineering*, *9*(22), 1–8.

Sierra, E. G., & Ramírez Arroyave, G. A. (2015). Low cost SDR spectrum analyzer and analog radio receiver using GNU radio, Raspberry Pi2 and SDR-RTL dongle. In *7th IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE Publisher. 10.1109/LATINCOM.2015.7430125

Simillion, H., Dolgikh, O., Terryn, H., & Deconinck, J. (2014). Atmospheric corrosion: A review focussed on modelling. *Corrosion Reviews*, 1–42.

Simoniot. (2020, Nov 20). *The Rise of IoT: The History of the Internet of Things*. https://www.simoniot.com/history-of-iot/

Singh, D., Tripathi, G., & Jara, A. J. (2014, March). A survey of Internet-of-Things: Future vision, architecture, challenges and services. In 2014 IEEE world forum on Internet of Things (WF-IoT) (pp. 287-292). IEEE.

Singh, R. (2012). *Applied Welding Engineering: Processes, Codes And Standards*. Elsevier Inc.

Skeppstedt, M. (2011). Negation detection in Swedish clinical text: An adaption of NegEx to Swedish. *Journal of Biomedical Semantics*, *2*(Suppl 3). doi:10.1186/2041-1480-2-S3-S3 PMID:21992616

Skotnicki, T., Hutchby, J. A., King, T. J., Wong, H. S., & Boeuf, F. (2005). The end of CMOS scaling: Toward the introduction of new materials and structural changes to improve MOSFET performance. *IEEE Circuits and Devices Magazine*, *21*(1), 16–26.

Soares, G., Garbatov, Y., & Zayed, A. (2011). Effect of Environmental Factors on Steel Plae Corrosion under marine Immersion Conditions. *Corrosion Engineering, Science and Technology*, *46*(4), 524–541. doi:10.1179/147842209X12559428167841

Song, J., & Ochiai, H. (2016). Performance Analysis for OFDM Signals With Peak Cancellation. *IEEE Transactions on Communications*, *64*(1), 261–270. doi:10.1109/TCOMM.2015.2502585

Soska, K., & Christin, N. (2014). Automatically detecting vulnerable websites before they turn malicious. *23rd USENIX Security Symposium (USENIX Security 14)*, 625–640.

Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., De Souza, L. M. S., & Trifa, V. (2009, July). *SOA-based integration of the internet of things in enterprise services. In 2009 IEEE international conference on web services*. IEEE.

Stack, M. M., Chacon-Nava, J., & Stott, F. H. (1995). Relationship Between the Effects of Velocity and Alloy Corrosion Resistance in Erosion-Corrosion Environment at Elevate Temperatures. *Wear*, *180*(1-2), 91–99. doi:10.1016/0043-1648(94)06536-5

Steber, G. R. (2020). An ultra low cost vector network analyser. *QEX*, 3–9.

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964–975. doi:10.1016/j.future.2016.11.031

Stewart, R. W., Crockett, L., Atkinson, D., Barlee, K., Crawford, D., Chalmers, I., Mclernon, M., & Sozer, E. (2015). A low-cost desktop software defined radio design environment using MATLAB, Simulink, and the RTL-SDR. *IEEE Communications Magazine*, *53*(9), 64–71. doi:10.1109/MCOM.2015.7263347

Stoyanov, V., Cardie, C., & Wiebe, J. (2005). Multi-perspective question answering using the OpQA corpus. *HLT '05: Proceedings of the conference on Human Language Technology and Empirical Methods in Natural Language Processing*, 923–930. 10.3115/1220575.1220691

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., Whitley, S. M., & Wolf, R. D. (2017). *Finding cyber threats with ATT&CK-based analytics.* The MITRE Corporation, Technical Report No. MTR170202.

Subir, P. (2010). Estimation of Corrosion Rate of Mild Steel in Sea Water and Application of Genetic Algorithms to Find Minimum Corrosion Rate. *Canadian Metallurgical Quarterly*, *41*(1), 1–8.

Tactic, A. (2017). *Techniques and Common Knowledge*. ATT&CK.

Taghavi-Zenouz, R., Salari, M., & Etemadi, M. (2008). Prediction of Laminar, Transitional and Turbulent Flow Regimes Based on Three Equation k-w Turbulence Flow. *Aeronautical Journal*, *112*(1134), 469–476. doi:10.1017/S0001924000002438

Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-376). IEEE.

Taunk, K. (2019). Article. *2019 International Conference on Intelligent Computing and Control Systems, ICCS 2019, Iciccs*, 1255–1260.

Taur, Y., Buchanan, D. A., Chen, W., Frank, D. J., Ismail, K. E., Lo, S. H., ... Wong, H. S. (1997). CMOS scaling into the nanometer regime. *Proceedings of the IEEE*, *85*(4), 486–504.

Taylor, L. (2011, October). Alliance, and Zig Bee, Interconnecting ZigBee & M2M networks. In *Proc. ETSI M2M Workshop* (pp. 1-18). Academic Press.

Taylor, J. M., & Sharif, H. R. (2017). Security challenges and methods for protecting critical infrastructure cyber-physical systems. *Selected Topics in Mobile and Wireless Networking (MoWNeT), 2017 International Conference On*, 1–6.

Tellado, J. (1999). *Peak to Average Ratio Reduction for Multi-carrier Modulation* [PhD Thesis]. Stanford University, Stanford, CA, USA.

Tellado, J., & Cioffi, J. M. (1998). Peak power reduction for multicarrier transmission. *Proc. IEEE Global Communications Conference (CLOBECOM).*

Thayananthan, V. (2019). Healthcare management using ICT and IoT based 5G. *International Journal of Advanced Computer Science and Applications*, *10*(4), 305–312. doi:10.14569/IJACSA.2019.0100437

The Materials Information Society. (2006). *Corrosion of Weldments* (J. R. Davis, Ed.). ASM International.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. doi:10.1016/j.cose.2017.09.001

Turian, R. M., Hsu, F. L., & Ma, T. W. (1987). Estimation of the Critical Velocity in Pipeline Flow of Slurry. *Powder Technology*, *51*(1), 35–47. doi:10.1016/0032-5910(87)80038-4

Ukhurebor, K., Batubo, T., Abiodun, I., & Enoyoze, E. (2017). The Influence of Air Temperature on the Dew Point Temperature in Benin City, Nigeria. *Journal of Applied Science & Environmental Management*, *21*(4), 657–660. doi:10.4314/jasem.v21i4.5

Ullah, F., Naeem, M. R., Mostarda, L., & Shah, S. A. (2021). Clone detection in 5G-enabled social IoT system using graph semantics and deep learning model. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3115–3127. Advance online publication. doi:10.100713042-020-01246-9

Unified Medical Language System (UMLS) at National Library of Medicine. (n.d.). Retrieved March 26, 2022, from https://www.nlm.nih.gov/research/umls/index.html

van Nee, R., & de Wild, A. (n.d.). Reducing the peak-to-average power ratio of OFDM. *VTC '98. 48th IEEE Vehicular Technology Conference. Pathway to Global Wireless Revolution, 3*, 2072–2076. 10.1109/VETEC.1998.686121

Vangelista, L., Zanella, A., & Zorzi, M. (2015, September). Long-range IoT technologies: The dawn of LoRa. In *Future access enablers of ubiquitous and intelligent infrastructures* (pp. 51–58). Springer.

Vargas, D. C. Y., & Salvador, C. E. P. (2016). Smart IoT gateway for heterogeneous devices interoperability. *IEEE Latin America Transactions*, *14*(8), 3900–3906.

Veeramachaneni, K., Arnaldo, I., Korrapati, V., Bassias, C., & Li, K. (2016). AI^ 2: training a big data machine to defend. *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 49–54.

Vidatronic Announces Series of Integrated Power Management Unit (PMU) IP Cores Optimized for Augmented/Virtual Reality Applications. (2021) Retrieved December 10, 2021 from https://www.vidatronic.com/vidatronic-announces-series-of-integrated-power-management-unit-pmu-ip-cores-optimized-for-augmented-virtual-reality-applications/

Wada, S., & Watanalm, W. (1987). *Solid gerlicle erosion in ~itte materials Part 3. The intersection with hi.ella[pl~pertles of target and th~z of impinginement particles on erosion wear mechanism.* Yogyo-Kyokai shL.

Wang, Z., Won Chung, J., Jiang, X., Cui, Y., Wang, M., & Zheng, A. (2018). Machine Learning-Based Prediction System For Chronic Kidney Disease Using Associative Classification Technique. *International Journal of Engineering & Technology, 7*(4.36), 1161. doi:10.14419/ijet.v7i4.36.25377

Wang, C.-L., & Yuan, O. (2005). Low-complexity selected mapping schemes for peak-to-average power ratio reduction in OFDM systems. *IEEE Transactions on Signal Processing*, *53*(12), 4652–4660. doi:10.1109/TSP.2005.859327

Wang, D., Chen, D., Song, B., Guizani, N., Yu, X., & Du, X. (2018). From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies. *IEEE Communications Magazine*, *56*(10), 114–120.

Wang, L., & Tellambura, C. (2008). Analysis of Clipping Noise and Tone-Reservation Algorithms for Peak Reduction in OFDM Systems. *IEEE Transactions on Vehicular Technology*, *57*(3), 1675–1694. doi:10.1109/TVT.2007.907282

Wang, X., Tjhung, T. T., & Ng, C. S. (1999). Reduction of peak-to-average power ratio of OFDM system using a companding technique. *IEEE Transactions on Broadcasting*, *45*(3), 303–307. doi:10.1109/11.796272

Wang, X., Tjhung, T. T., & Ng, C. S. (1999). Reply to the comments on "Reduction of peak-to-average power ratio of OFDM system using a companding technique." *IEEE Transactions on Broadcasting*, *45*(4), 420–422. doi:10.1109/11.825538

Weyrich, M., & Ebert, C. (2015). Reference architectures for the internet of things. *IEEE Software*, *33*(1), 112–116. doi:10.1109/MS.2016.20

Wharton, J. A., & Wood, R. K. (2004). Influence of Flow Conditions on the Corrosion of AISI 304L Stainless Steel. *Wear*, *256*, 525–536.

Wilkie, F. G., & Kitchenham, B. A. (2000). Coupling measures and change ripples in C++ application software. *Journal of Systems and Software*, *52*(2-3), 157–164. doi:10.1016/S0164-1212(99)00142-9

Wilkinson, T. A., Jones, A. E., & Barton, S. K. (1994). Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes. *Electronics Letters*, *30*(25), 2098–2099. doi:10.1049/el:19941423

Winkelaar, A. (2009). *Coating Basics*. Vincentz Network, GmbH & Co. KG.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. doi:10.1016/j.chb.2008.04.005

Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-484). IEEE.

Wu, C. Y., Lou, J. C., & Deng, Z. B. (2018, April). An ultra-low power capacitor-less LDO for always-on domain in NB-IoT applications. In *2018 IEEE International Conference on Applied System Invention (ICASI)* (pp. 137-140). IEEE.

Wu, W., Kang, R., & Li, Z. (2015). Risk assessment method for cyber security of cyber physical systems. *Reliability Systems Engineering (ICRSE), 2015 First International Conference On*, 1–5.

Wu, Y., & Zou, W. Y. (1995). Orthogonal frequency division multiplexing: A multi-carrier modulation scheme. *IEEE Transactions on Consumer Electronics*, *41*(3), 392–399. doi:10.1109/30.468055

Xu, Y., Hu, G., You, L., & Cao, C. (2021). A Novel Machine Learning-Based Analysis Model for Smart Contract Vulnerability. *Security and Communication Networks*, *2021*, 2021. doi:10.1155/2021/5798033

Yamazaki, T. (2006, November). Beyond the smart home. In *2006 International Conference on Hybrid Information Technology* (Vol. 2, pp. 350-355). IEEE. 10.1109/ICHIT.2006.253633

Yang, L., Chen, R. S., Siu, Y. M., & Soo, K. K. (2006). PAPR Reduction of an OFDM Signal by Use of PTS With Low Computational Complexity. *IEEE Transactions on Broadcasting*, *52*(1), 83–86. doi:10.1109/TBC.2005.856727

Yang, Z., Fang, H., & Pan, C. (2005). ACE With Frame Interleaving Scheme to Reduce Peak-to-Average Power Ratio in OFDM Systems. *IEEE Transactions on Broadcasting*, *51*(4), 571–575. doi:10.1109/TBC.2005.851697

Yassein, M. B., Aljawarneh, S., & Al-Sadi, A. (2017, November). Challenges and features of IoT communications in 5G networks. In *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)* (pp. 1-5). IEEE. 10.1109/ICECTA.2017.8251989

Yen, T.-F., Heorhiadi, V., Oprea, A., Reiter, M. K., & Juels, A. (2014). An epidemiological study of malware encounters in a large enterprise. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 1117–1130. 10.1145/2660267.2660330

Yeole, A. S., & Kalbande, D. R. (2016, March). Use of Internet of Things (IoT) in healthcare: A survey. In *Proceedings of the ACM Symposium on Women in Research 2016* (pp. 71-76). 10.1145/2909067.2909079

Yesmin, T., Agasti, S., & Chakrabarti, K. (2022). 5G Security and Privacy Issues: A Perspective View. In *ICT with Intelligent Applications* (pp. 89–98). Springer.

Yi, D. L., & Liang, D. (2010). A survey of the internet of things. *Proc. of ICEBI.*

Yoo, H., Han, S., & Chung, K. (2020). A frequency pattern mining model based on deep neural network for real-time classification of heart conditions. *Healthcare (Switzerland)*, *8*(3), 234. Advance online publication. doi:10.3390/healthcare8030234 PMID:32722657

You, K. Y. (2017). Materials characterization using microwave waveguide system. In S. Goudos (Ed.), *Microwave systems and applications* (pp. 341–358). IntechOpen. doi:10.5772/66230

You, K. Y., Derek Ng, Y. S., Lee, C. Y., Abbas, Z., Cheng, E. M., Lee, Y. S., & Lee, K. Y. (2017). Low-cost vector network analyser for communication devices testing – brief review. *International Journal of Advances in Microwave Technology*, *2*(1), 93–97.

Young, T., Hazarika, D., Poria, S., & Cambria, E. (2018). Recent trends in deep learning based natural language processing. *IEEE Computational Intelligence Magazine*, *13*(3), 55–75. doi:10.1109/MCI.2018.2840738

Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., & Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture*, *98*, 289–330. doi:10.1016/j.sysarc.2019.02.009

Zabre, S., Palicot, J., Louet, Y., & Lereau, C. (2006). SOCP Approach for OFDM Peak-to-Average Power Ratio Reduction in the Signal Adding Context. *2006 IEEE International Symposium on Signal Processing and Information Technology*, 834–839. 10.1109/ISSPIT.2006.270914

Zadeh, L. A. (1988). Fuzzy logic. *Computer*, *21*(4), 83–93. doi:10.1109/2.53

Zahoor, F., Hussin, F. A., Khanday, F. A., Ahmad, M. R., Mohd Nawi, I., Ooi, C. Y., & Rokhani, F. Z. (2021). Carbon nanotube field effect transistor (cntfet) and resistive random-access memory (rram) based ternary combinational logic circuits. *Electronics (Basel)*, *10*(1), 79.

Zelinka, S. L., Glass, S. V., & Derome, D. (2014). The Effect of Moisture Content on the Corroson of Fasteners Embedded in Wood Subjected to Alkaline Copper Quaternary Treatment. *Corrosion Science*, *83*, 67–74. doi:10.1016/j.corsci.2014.01.044

Zemrane, H., Abbou, A. N., Baddi, Y., & Hasbi, A. (2018, November). Wireless Sensor Networks as part of IOT: Performance study of WiMax-Mobil protocol. In *2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)* (pp. 1-8). IEEE.

Zeng, D., Guo, S., & Cheng, Z. (2011). The web of things: A survey. *Journal of Communication*, *6*(6), 424–438.

Zhang, Y., Yongacoglu, A., Chouinard, J.-Y., & Zhang, L. (n.d.). OFDM peak power reduction by sub-block-coding and its extended versions. *1999 IEEE 49th Vehicular Technology Conference, 1*, 695–699. 10.1109/VETEC.1999.778254

Zhang, L., Chan, M., & He, F. (2010, December). The impact of device parameter variation on double gate tunneling FET and double gate MOSFET. In *2010 IEEE International Conference of Electron Devices and Solid-State Circuits (EDSSC)* (pp. 1-4). IEEE.

Zhong, M., Yang, Y., Yao, H., Fu, X., Dobre, O. A., & Postolache, O. (2019). 5G and IoT: Towards a new era of communications and measurements. *IEEE Instrumentation & Measurement Magazine*, *22*(6), 18–26.

Zhou, Y., & Jiang, T. (2009). A novel clipping integrated into ACE for PAPR reduction in OFDM systems. *2009 International Conference on Wireless Communications & Signal Processing*, 1–4. 10.1109/WCSP.2009.5371552

Zhuang, Y., Liu, Z., Qian, P., Liu, Q., Wang, X. & He, Q. (n.d.). *Smart contract vulnerability detection using graph neural networks*. Academic Press.

Ziegler, S., Skarmeta, A., Kirstein, P., & Ladid, L. (2015, December). Evaluation and recommendations on IPv6 for the Internet of Things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 548-552). IEEE. 10.1109/WF-IoT.2015.7389113

Zimmermann, H.-J. (2011). *Fuzzy set theory—and its applications*. Springer Science & Business Media.

About the Contributors

Augustine O. Nwajana holds a PhD in Electrical and Electronic Engineering from the University of East London UK, and a research CPD certificate in Practical Antenna Design: from Theory to Practice, from the University of Oxford UK. He was with Siemens AG as a Telecoms Engineer for four years (2005 to 2009), where his experience spanned many countries including USA, UK, UAE, Germany, South Africa, Ghana, and Nigeria. He was also with Coventry University (as an associate lecturer) and with University of East London (as a part-time lecturer). Dr. Nwajana is currently a senior lecturer with the University of Greenwich where his current research interest includes RF energy harvesting/scavenging; battery-less RF/microwave systems; passive RF/microwave devices, etc. He has authored/co-authored five books, several journal articles, book chapters, and conference papers. Augustine is currently serving as editor for IGI Global USA, and Electronics MDPI Switzerland. He has served as keynote speaker and TPC member for several conferences. He is a Senior Member of the IEEE, and a Fellow of the UK Higher Education Academy. He was a recipient of the Federal Government of Nigeria Scholarship Award.

* * *

Umang Garg received the master degree from AKTU, Lucknow, India. He is working as an Assistant Professor in Graphic Era Hill University, Dehradun since 2017. His area of Interest includes IoT Security, Intrusion Detection System for IoT, and Machine Learning.

Neha Gupta received the master degree from AKTU, Lucknow, India. He is currently pursuing PhD from Graphic Era Deemed to be University, Dehradun. His area of Interest includes IoT Security, Intrusion Detection System for IoT, 5G, and Machine Learning.

Aymen Hlali received the master's degree in electrical engineering and the Ph.D. degree in electronics from the National Engineering School of Carthage, Tunisia, in 2017 and 2020, respectively. He is currently an Assistant Professor with the National Engineering School of Carthage and also a Researcher with the Research Laboratory Smart Electricity and ICT, Tunisia. His research interests include electromagnetic microwave circuit modeling and numerical methods, and components based on graphene.

Guan Yue Hong is an associate professor of Computer Science at Western Michigan University. She received her Ph.D. in software engineering from National University of Singapore. Her research interests include reliable and trustworthy AI, novel machine learning paradigms, and smart cyber-physical-human systems. She received several grants and awards in support of her scholarly activities. She has published over 70 papers in leading international journals and conferences, e.g. IEEE Trans. Affective Computing, IEEE Trans. Consumer Electronics, and IEEE Trans. IT in Biomedicine. Her published papers have attracted over a thousand scientific citations.

Pradeep Juneja is presently working as Professor in School of Engineering at Graphic Era University, Dehradun, where he joined as lecturer in July 2004. He completed PhD from IIT Roorkee in the area of Multivariable Constrained Complex Predictive Process Control engineering and M.Tech. and B.Tech. from DAVV Indore and MJPRU, Bareilly respectively. He has 20 years of teaching and research experience. 18 M.Tech dissertations and 4 P.hD. thesis are awarded under his guidance. He has published more than 121 research publications in reputed journals and conference proceedings including those in Taylor and Francis, SCI, Scopus, Springer, Elsevier and IEEExplore database.

Jyoti Kandpal received the B.Tech. degree in electronics and communication engineering from Bipin Chandra Tripathi, Kumaon Engineering College, Dwarahat, India, in 2012, and the M.Tech. degree in VLSI design from the Department of Electronics and Communication Engineering, Uttarakhand Technical University, Dehradun, India, in 2015. She received the Ph.D. degree in Electronics and Communication Engineering from the College of Technology, G. B. Pant University, Pantnagar, India, in 2021. Since March 2021, she has been working as a Research Engineer with NIT Arunachal Pradesh, India. Her research interest includes VLSI design and high-performance digital circuits design.

Yeng Seng Lee received his Bachelor's degree Communication Engineering (Honours) degree and Ph.D. in communication engineering from the School of Computer and Communication Engineering at UniMAP, Malaysia in 2012 and 2016, respectively. He is currently a senior lecturer at the Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP). He is also a member of IET, IEEE, MBOT, BEM and a fellow member of Advanced Communication Engineering, centre of excellence. From 2012 up until 2021, He has authored and co-authored more than 80 journal and conference papers. Besides, he also has received 42 awards from national and international exhibitions. His research interests include Food security, Dielectric Material Characterization, Microwave Absorber, Electromagnetic, Antenna, Microwave Measurement, and Frequency Selective Surface (FSS).

Richard I. Otuka (Member, IEEE) received the B.Sc. and M.Sc. degrees in information systems and the Ph.D. degree in computer science from the School of Architecture, Computing, and Engineering, University of East London (UEL). He is currently a lecturer at the department of computing, Nottingham Trent University, UK. He is also a Researcher in cloud computing, knowledge -based system with ontology, business intelligence and cyber security. He has received many academic awards for innovative teaching and student support.

Payaswini P. received M.Sc. degree in Computer Science in 2010 and a PhD degree in Computer Science in 2016 from Mangalore University. She is currently working as an Assistant Professor of Computer Science & Technology at Goa University. She worked as a Project Fellow under UGC Major research project in the area of Mobility managements in 4G networks. She was the recipient of the DST INSPIRE scholarship. She has 8 publications in peer reviewed journals and international conferences. Her current research interests include Mobile networks, Cloud computing, and Internet of Things.

Sachin Sharma is currently an Associate Dean, International Affairs and Associate Professor, Department of Computer Science and Engineering at Graphic Era Deemed to be University, Dehradun, UK, India. He is also Co-founder and Chief Technology officer (CTO) of IntelliNexus LLC, Arkansas, USA based company. He also worked as a Senior Systems Engineer at Belkin International, Inc., Irvine, California, USA for two years. He received his Philosophy of Doctorate (Ph.D.) degree in Engineering Science and Systems specialization in Systems Engineering from University of Arkansas at Little Rock, USA with 4.0 out 4.0 GPA and M.S. degree in Systems engineering from University of Arkansas at Little Rock with 4.0 out 4.0 GPA. His research interests include wireless communication networks, IoT, Vehicular ad hoc networking and network security.

Abhay Kumar Singh received the B.Tech. degree in electronics and communication engineering from S.L.S.E.T, Kichha, India, in 2013, and the M.Tech.

degree in Digital Communication Bipin Chandra Tripathi, Kumaon Engineering College, Dwarahat, India, in 2016. He is currently pursuing the Ph.D. degree with the College of Technology, G. B. Pant University of Agriculture and Technology, Pantnagar, India. His current research interests include Microwave Antenna for Wireless Communication; Terahertz Antenna for Compact and Efficient Source; Nano Structures and Nano Antenna for Optical Applications.

Kok Yeow You was born in 1977. He obtained his B.Sc. Physics (Honours) degree in Universiti Kebangsaan Malaysia (UKM) in 2001. He pursued his M.Sc. in Microwave at the Faculty of Science in 2003 and his Ph.D. in Wave Propagation at the Institute for Mathematical Research in 2006 in Universiti Putra Malaysia (UPM), Serdang, Selangor, Malaysia. Recently, he is a senior lecturer at the School of Electrical Engineering, Faculty of Engineering, Universiti Teknologi Malaysia (UTM), Skudai, Johor, Malaysia. His main personnel research interest is in the theory, simulation, and instrumentation of electromagnetic wave propagation at microwave frequencies focusing on the development of microwave passive devices and sensors for medical and agricultural applications.

Hassen Zairi (Senior Member, IEEE) is currently a Professor with the National Engineering School of Carthage, Tunisia, where he is also the Director. His research interests include microwave antennas and circuits modeling, numerical methods for the analysis of microwave, and millimeter-wave circuits.

Index