IIoT Communication Protocols Compatibility and Security An In-depth Review

Maryam Karimi[1] and Roland Shaefer[1]

[1]Affiliation not available

March 25, 2025

IIoT Communication Protocols Compatibility and Security An In-depth Review

Maryam Karimi, *Senior member, IEEE,* Automation, Digitalization & Cyber Research, FM
maryam.karimi@fmglobal.com
Roland Shaefer, Automation, Digitalization & Cyber Research, FM, roland.shaefer@fmglobal.com

***Abstract*—This paper presents an effort to taxonomize and categorize common protocols of the Industrial Internet of Things (IIoT) and their different versions based on their compatibility with other layer protocols. Through intensive research, the paper provides a comprehensive review of the telecommunication network, Industrial Control Systems (ICS), and Internet of Things (IoT) standards and protocols, highlighting their technical importance in modern industrial applications. The paper first analyzes the components of IIoT and then focuses on the telecommunication network protocol used between those components. It depicts the compatibility of the most frequently used protocols in IIoT in different layers, using a structure based on TCP/IP and OSI reference models. This paper proposes a novel compatibility stack that can guide system designers and engineers in selecting the most appropriate communication protocols for their IIoT applications. Finally, the paper reviews the organizations involved in standardizing communication protocols. This contribution to the body of knowledge in IIoT provides a resource for researchers, engineers, and practitioners seeking to understand and implement IIoT technologies, communication protocols, and their compatibilities.**

***Index Terms*—Communication protocols and standards, ICS protocols, IoT protocols, Protocol compatibility stack, Industrial Internet of Things**

I. Introduction

THE Industrial Internet of Things (IIoT) is a dynamic and complex ecosystem of technologies that are designed to work together to improve intelligence, efficiency, and safety in industrial settings. By increasing connectivity between devices and systems, IIoT technologies can greatly reduce the time and costs associated with industrial processes. Furthermore, these integrated technologies can facilitate real-time monitoring and analytics, enabling organizations to identify and address issues before they become major problems and hence reduce the time and costs [Baudoin et al.(2021)]. Typical critical IIoT components for an effective industrial IoT architecture, consisting of multiple elements that work together to meet industrial needs. Common elements in IIoT networks including control systems, edge, cloud, connectivity, and security.

Industrial Control Systems (ICS) also called as Operational Technology (OT) are systems that use hardware and software to manage industrial equipment and processes. They require fast, real time communication for critical control messages; therefor, they are typically located on the perimeter. Industrial automation and control systems, such as PLC (Programmable Logic Controller), DCS (Distributed Control System), and SCADA (Supervisory Control and Data Acquisition), play crucial roles in managing various processes. PLCs automate industrial processes and monitor inputs/outputs in critical operations, DCSs automate complex tasks using a network of controllers, and SCADAs remotely monitor and control processes while enabling human-machine interaction. These systems collectively contribute to efficient, reliable, and safe operations.

Another typical element of the ICS is historian which is a software application or system designed to efficiently collect, store, and manage time-series data generated by industrial processes and equipment. With its high data ingestion rates, data compression, and advanced querying capabilities, the historian provides valuable insights into trends, patterns, and anomalies. These insights can be used for optimizing processes, enhancing equipment performance, and implementing predictive maintenance strategies. Depending on the specific architecture, requirements of the IIoT system, and security considerations, a historian can be located either at the edge, enabling faster data processing, or remotely in a centralized server or cloud environment, allowing for better data aggregation and analysis. Aggregated data from historians can be stored in the remote cloud server.

IIoT (Industrial Internet of Things) is an extension of ICS that leverages the power of connected devices to improve industrial processes by collecting, exchanging, and analyzing data and thus increasing efficiency and reliability. Hundreds or thousands of connected sensors and actuators in IIoT transmit data to a gateway with limited storage and processing resources. The gateway may offer real-time monitoring and Internet access. Data are then forwarded to the cloud through the Internet or other networks for storage and in-depth analysis, facilitating long-term monitoring and feedback to enhance business operations.

In IIoT, edge computing involves processing and analyzing data near its source, such as sensors and devices. The edge side features various sensors, including control and environmental sensors. The latter are designed to monitor and measure various environmental parameters such as temperature, while control sensors play a vital role in managing and regulating industrial processes, equipment, and systems by detecting changes in variables and making adjustments accordingly. Sensors exchange information with a gateway and interact with remote services via that gateway.

The gateway is a networking device (e.g., router, switch, firewall, or other middleboxes) that serves as an intermedi-

This paper was produced by department of Innovation and Future of Industry in Factory Mutual (FM) insurance company.
Manuscript received March 20

ary between different communication protocols, networks, or systems, enabling data transmission between them. It acts as an entry and exit point for data traffic and is responsible for converting and routing data packets between the source and destination devices. A gateway can perform several functions, such as protocol translation, data processing, implementing security measures such as encryption, authentication, and access control, and edge computing and data analysis and monitoring. A gateway can preprocess received data, summarizing it to reduce cost and time of data transmission and storage, before forwarding it to multiple destinations such as i) local historian for data storage, ii) a remote cloud server for further storage, processing, and data analyses, iii) a corporate network for monitoring purposes, or iv) a control system to enable automated decision-making and actions.

The cloud is generally referred to a server with high storage and processing resources. Cloud server can be owned by either the user or cloud service provider. Employing a cloud server, whether it is over the Internet or on a local server, provides the advantage of increased capacity of data storage, processing, and management as well as facilitating the use of advanced data analytics and machine learning methods. Key features of a quality remote cloud server include scalability, accessibility, cost-effectiveness, reliability, and robust security measures such as encryption, access control, and monitoring.

IIoT elements can use variety of communication protocols for on perimeter connections as well as communication with remote elements. There are multiple ways to categorize communication protocols based on security, range (for wireless protocols), routing algorithms, architecture, scalability, data rate, network topology, power consumption and many other factors. For example, in Ref. [Nguyen et al.(2015)] security protocols are categorized based on key bootstrapping, asymmetric key schemes, key transport, and RPKE (raw public key encryption), and these factors are used for analyzing their effectiveness in providing confidentiality, integrity, authentication, authorization, freshness, resilience, computation complexity, memory, scalability, and privacy protection. As another example, routing protocols can be categorized based on their objectives, architecture, power transmission method, whether they are fixed or adjustable, operation-based routing, and route selection method [Abdullah and Ehsan(2014)]. Some articles have focused on the coverage range of wireless protocols and categorized them [Mubashar et al.(2021)], [Erwinski et al.(2023)]. Researchers also have focused on wireless sensor network protocols and categorized them based on range data rate and applications [Henke(2022)], [Ghayvat et al.(2014)].

This paper aims to identify the most prevalent protocols in industrial use cases and their compatibility with each other as shown in Fig. 1 To achieve this goal, an in-depth investigation was conducted on the existing IIoT standards and protocols that are currently being utilized in various industries.

While previous research has been done on identifying prevalent protocols for IoT and IIoT applications, these studies are not as comprehensive as our work. For example, some previous work has focused on IoT protocols [Naik(2017)], [Larmo et al.(2018)], IoT wireless protocols [Newark(2023)], and the Mobile Multimedia All-IP Protocol Stack [Howie et al.(2004)]. In this work we take a deep dive into the compatibility and interoperability of protocols in industrial cases covering IT (Information Technology), ICS (Industrial Control Systems)/ OT (Operational Technology), and IoT (Internet of Things) protocols.

Through intensive research, we have taxonomized and categorized IIoT common protocols and their different versions based on the compatibility with other layer protocols. Fig. 1 presents a comprehensive overview of the most common protocols used in Industrial IoT, illustrating the layers they belong to and their compatibility with other layer protocols. The protocol layers are indicated on the left side of the image and are differentiated by color: green for Physical and Link layers, blue for the Network layer, orange for the Transport layer, and yellow for the Application layer.

Fig. 1 depicts the novelty of this paper; It was developed to show the compatibility of various protocols across different layers. Compatible protocols are presented one below the other. By referring to this figure, users can easily determine such compatibility, which is crucial in designing and implementing effective Industrial IoT communication systems. The rest of this paper provides the background on network stack models of the OSI standard model and TCP/IP model, and further investigates the protocols used in Fig. 1 in Sections III,IV,V and VI.

II. Communication Protocol Stack Background

The edge side features various sensors collecting and transmitting information to a gateway or historian, which may possess limited storage and processing capabilities for data management and network monitoring. Numerous wired and wireless communication protocols can be employed within the edge network. This section reviews the specifications of some of the most commonly used protocols. This section gives a brief overview of network models, followed by a brief discussion of various protocols, such as IT protocols, ICS protocols, IoT wireless protocols, and IoT application protocols. TCP/IP and OSI Reference Models (See Fig.2) are two widely known networking models that define how communication protocols and network systems interact and exchange data. Both models serve as a framework for understanding and implementing network communication, but they have different structures and origins [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)].

The OSI (Open Systems Interconnection) Reference Model is a seven-layer conceptual framework developed by the International Organization for Standardization (ISO) in the late 1970s and early 1980s. Its primary goal was to enable interoperability between different networking systems and provide a standard for developing communication protocols. The OSI model consists of seven layers including application, presentation, session, transport, network, data link and physical layer [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)]. These layers are briefly explained below.

- **Application Layer** provides the interface between the user applications and the network.

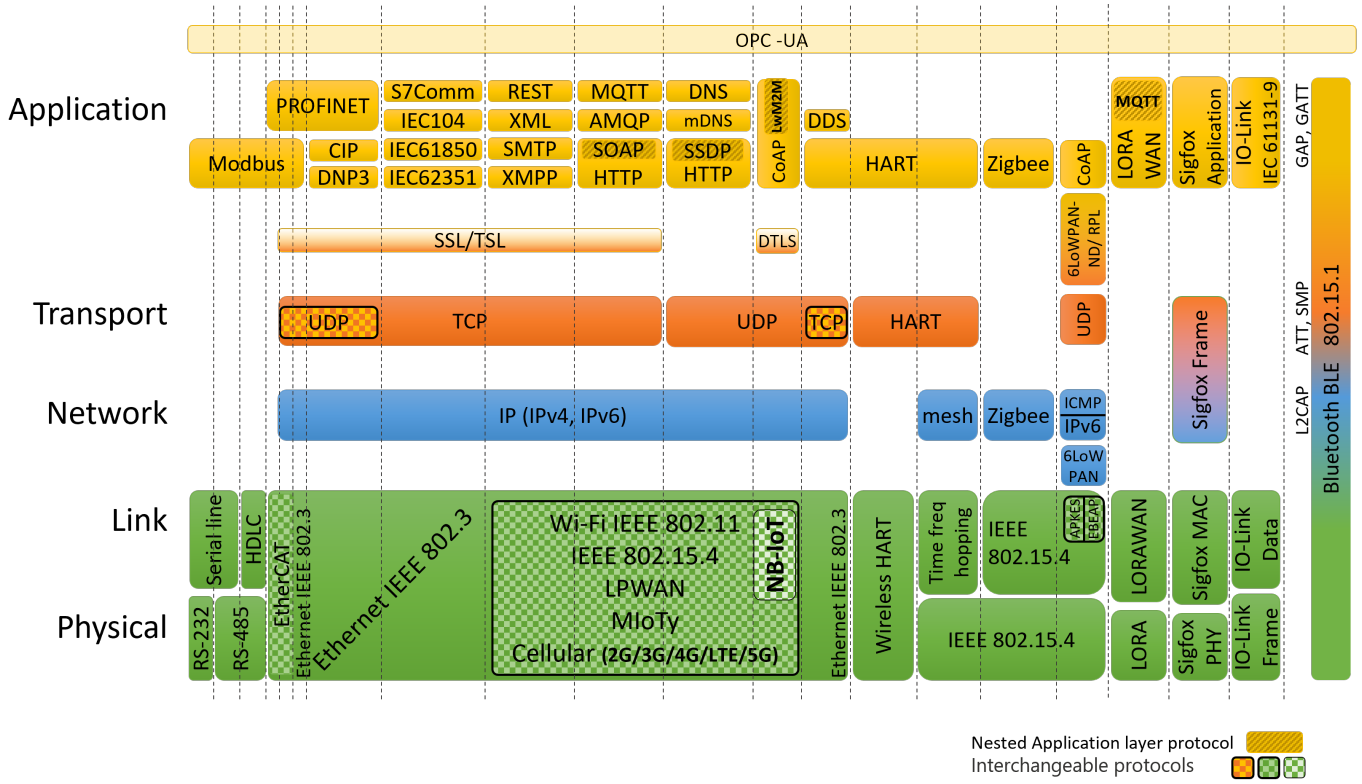

Fig. 1. Protocol compatibility stack

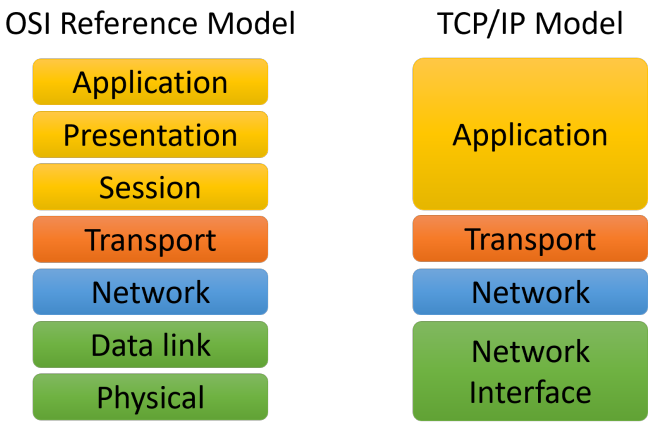

Fig. 2. OSI reference model vs TCP/IP model [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)]

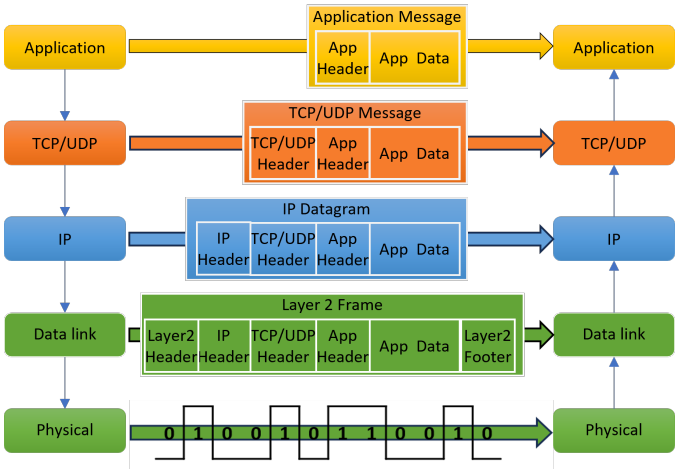

Fig. 3. Network encapsulation [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)]

- **Presentation Layer** is responsible for data representation, encryption, and compression.
- **Session Layer** manages the establishment, maintenance, and termination of connections between network devices.
- **Transport Layer** provides end-to-end communication services, including flow control, error detection, and connection management.
- **Network Layer** is responsible for routing and addressing data packets across networks.
- **Data Link Layer** is responsible for the reliable transmission of data frames between devices on a network.
- **Physical Layer** defines the physical characteristics of the network, such as voltage levels, timing, and signaling, to enable data transmission over a medium [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)].

The TCP/IP (Transmission Control Protocol/Internet Protocol) model, also known as the Internet Protocol Suite, is a set of communication protocols used on the Internet and other similar networks. Developed by the U.S. Department of Defense (DoD) in the 1970s, it became the foundation for the

modern Internet. The TCP/IP model consists of four layers including application layer, network layer (IP), transport layer (TCP/UDP), data link layer (MAC) and physical layer (refer to Fig. 1).

As shown in Fig 3, In the networking protocol stack, each layer wraps data from the layer above it with a header that contains necessary protocol information, such as version, sender and receiver address, coding, flags, length, checksum, etc., before passing the packet down to the next layer. This process is also known as data encapsulation. However, it is important to note that not all protocols are compatible with each other since certain protocols may only work with specific protocols from other layers. The compatibility between protocols is discussed in detail in Section III with focus on IT protocols, Section IV with focus on IoT application protocols, Section V with focus on Wireless protocols mostly in Data Link and Physical layer and Section VI with focus on ICS and Industrial protocols.

III. Internet Protocols and Standards

The most common internet protocols for each layer are explained below. In IT networks Ethernet and UDP/TCP/IP are used as media and transport for the backbone network and supports different application protocols for different purposes.

A. Internet Backbone

The Transmission or Transport Layer is responsible for segmenting and reassembling data into packets and providing error detection mechanisms. Common protocols are as follows:

- **TCP** (Transmission Control Protocol) ensures delivery by queuing sent packets until receiving an acknowledgement for each sent packet and resend if the acknowledgment was not received after a certain wait time [Kurose and Ross(2010)].
- **UDP** (User Datagram Protocol) is a transmission protocol for time sensitive applications with no delivery assurance [Kurose and Ross(2010)].

The Network Layer protocol is responsible for routing data packets between networks and ensuring that they reach their destination by selecting the most efficient path. The most common network layer is IP.

- **IP**(Internet Protocol) is responsible for addressing and routing data packets between devices on a network [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)].

The Data Link Layer protocol transmits data frames between adjacent nodes, providing mechanisms for error detection and correction, flow control, and ordered delivery, while the physical layer protocol transmits raw bitstream over the physical medium.

- **Ethernet** is a common wired networking technology used in Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), etc. Ethernet is also known as IEEE802.3. Ethernet connections have been established using twisted pairs, copper, or optic cable [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)], [Kurose and Ross(2010)].

B. Application Layer

The Application Layer is responsible for providing services and interfaces for end-users to interact with network resources and data. This layer has a variety of protocols that cover different types of applications. Some common protocols include:

HTTP (Hypertext Transfer Protocol) transfers data on the World Wide Web [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)], HTTP/S is an application layer protocol that operates over the internet protocol TCP/IP. It is used for web applications and typically runs on port 80. HTTPS is an extension of HTTP that uses encryption for secure communication and runs on port 443. Previously, HTTPS used SSL, which is not secure; therefore, it is not supported in many modern web browsers. Instead, HTTPS uses TLS (Transport Layer Security), which provides 256-bit encryption, a 3-step handshake, and HMAC and AEAD for message authentication. HTTPS provides authentication using X.509 certificates to authenticate the server and sometimes clients, as well as privacy and integrity for the transmitted data [Naik(2017)], [Friedl et al.(2014)], [Gourley and Totty(2002)].

TLS/SSL (Transport Layer Security/Secure Sockets Layer) are cryptographic protocols designed to provide secure communication by encrypting data and provide authentication, integrity, and confidentiality. There is debate about which layers of the OSI model these protocols belong to since they incorporate aspects of the Presentation Layer (Layer 6), Session Layer (Layer5) and Transport Layer (Layer 4). SSL is not secure and is prone to attacks. SSL provides 128-bit encryption, a 2-step handshake, and weak hash functions for message authentication. TLS supports 256-bit encryption and provides stronger security through a 3-step handshake and using stronger hash functions for message authentication [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)].

DNS (Domain Name System) translates human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) that computers use to identify each other on the network. DNS operates as an application layer protocol over TCP/IP and typically runs over UDP on port 53, using TCP for tasks requiring reliable transmission, such as zone transfers. DNS functions through a hierarchical structure, involving root servers, top-level domain (TLD) servers, authoritative servers, and recursive resolvers. When a user enters a domain name, a DNS query is generated, and the recursive resolver contacts various DNS servers to resolve the name into an IP address. DNSSEC (DNS Security Extensions) enhances security by providing data integrity and authentication through digital signatures and a public key infrastructure (PKI) [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)].

SMTP (Simple Mail Transfer Protocol) is used for sending email messages over the network. SMTP operates as an application layer protocol over the TCP/IP suite, typically running on port 25. For secure transmission, SMTPS uses port 465, and STARTTLS can upgrade an existing insecure connection to a secure one on port 587. SMTP works by

transferring email messages between mail servers using a process called store-and-forward. It initiates a connection to the recipient's mail server, where the message is then relayed to the recipient's mailbox. To enhance security, SMTPS (SMTP Secure) utilizes SSL/TLS for encryption, ensuring that email content and credentials are protected during transmission. Authentication mechanisms such as SMTP AUTH further secure the protocol by requiring users to authenticate with the mail server before sending emails, preventing unauthorized access and reducing spam [Cisco Systems(2023)], [Tanenbaum and Wetherall(2010)], [Peterson and Davie(2007)].

XML stands for eXtensible Markup Language, which is a markup language used for encoding documents in a format that is both human-readable and machine-readable. It is a widely used standard for data exchange between different applications and platforms. XML uses tags to define elements, attributes, and values within a document. These tags can be customized to define new data types that are specific to the needs of an application or domain. XML is often used to represent structured data, such as configuration files, web services, and data exchange formats. While there are alternatives to XML, such as JSON and YAML, XML remains a popular choice for many applications and systems due to its versatility, extensibility, and widespread support [Harold and Means(2004)].

SOAP (Simple Object Access Protocol) is a light-weight XML-based messaging protocol used for exchanging structured information between distributed and decentralized web services. It operates in a request-response model, where a SOAP message is sent from a client to a server, and the server sends back a response message. SOAP messages can be transported using protocols such as HTTP. SOAP provides a standardized way of exchanging data between different systems, and it supports a wide range of data types and structures. It also provides built-in support for encryption, digital signatures, and transaction management, making it a secure choice for enterprise-level applications. It supports WS (Web Services) and SSL (Secure Sockets Layer) for secure communication [Hirsch et al.(2007)].

RESTAPI (Representational State Transfer Application Programming Interface) is a web-based software architecture that uses HTTP protocol to enable communication between client and server applications. It provides a set of guidelines for building scalable, modular, and flexible web services that can be accessed over the Internet. RESTAPIs use HTTP methods like GET, POST, PUT, DELETE, etc., to perform operations on resources, which can be represented in different formats like XML, JSON, or HTML. REST APIs are stateless, meaning that each request contains all the information necessary to complete the request. This makes them highly scalable and easy to maintain [Masse(2011)].

IV. IoT Application Protocols

The most commonly used IoT Application Layer protocols are explained in this section, refer to Fig. 1.

MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol that uses a publish and subscribe model for remote communication. It is designed for use in high-latency, low-bandwidth, and unreliable networks, making it ideal for IoT and M2M (machine-to-machine) communication. MQTT scales to millions of devices and works over TCP, with a broker responsible for communication between publishers and subscribers. The broker stores and forwards messages, filters topics, provides security features, and ensures Quality of Service (QoS). MQTT provides various authentication techniques and encryption methods based on TLS. MQTT is simple and lightweight and is known for its low power consumption, making it suitable for use in embedded systems. It is widely used in industries like automotive, manufacturing, telecommunications, and smart homes for real-time data transmission and remote monitoring [Naik(2017)], [OASIS(2023)], [Kapoor and Kaur(2022)].

In Fig. 1, MQTT is shown as an Application Layer protocol. MQTT can work with TCP at the Transport Layer, IP at the Network Layer, and Ethernet (as well as Wi-Fi, LTE, IEEE 802.15.4, LPWAN) at the Physical and Link Layers. Additionally, as shown on the right side of the image, MQTT is compatible with LoRa and LoRaWAN.

AMQP (Advanced Message Queuing Protocol) is a message-oriented protocol that supports both point-to-point and publish-and-subscribe communication models. It uses a streamed binary messaging system to ensure interoperability in multi-client environments. AMQP uses a streamed binary messaging system to ensure interoperability in multi-client environments and operates over TCP as the default transport protocol, with TLS/SSL and SASL for security authentication and encryption. A broker is responsible for exchanging messages between publishers and subscribers. The broker has a separate queue for each publisher, and subscribers can receive messages from multiple queues. AMQP provides delivery guarantees such as "unsettled" (not reliable) and "settled" (reliable) formats, offering different levels of Quality of Service (QoS). Compared to MQTT, AMQP has higher bandwidth but slower speed. It also provides delivery guarantees such as "at most once," "at least once," and "exactly once." This makes it suitable for use in applications that require reliable and secure messaging [Gourley and Totty(2002)], [Kapoor and Kaur(2022)].

CoAP (Constrained Application Protocol) is a lightweight request-response web transmission protocol designed for machine-to-machine (M2M) communication and supports both client-to-server and server-to-server communications. It is used to enable communication between devices with limited resources, such as sensors, actuators, and other IoT devices. CoAP works over UDP, which makes it ideal for low-power and low-latency networks. It also supports multicast communication, allowing one message to be sent to multiple devices simultaneously. CoAP has a very low overhead, making it suitable for devices with limited memory and processing power. Its messages are easily translatable to HTTP, which allows integration with existing web-based systems. CoAP offers built-in support for resource discovery, caching, and security, including the use of **DTLS** and safeguards for UDP implementations of TLS, making it a secure and efficient protocol for M2M communication [Naik(2017)], [Gourley and Totty(2002)].

LwM2M (Lightweight Machine to Machine) protocol is used for seamless and efficient communication between IoT devices. It is simple, secure, and resource-efficient, leveraging the Constrained Application Protocol (CoAP) and offering various data models for device management, data reporting, and remote configuration. LwM2M is built on CoAP and thus uses UDP for faster transmission. It provides end-to-end security through DTLS and uses a standardized object model for simplified device management. The protocol defines four interface types for communication and accommodates devices with limited processing power, memory, and battery life, as well as ensuring interoperability between devices from different manufacturers [Alliance(2017)].

DDS (Data Distribution Service) is a data-centric standard protocol defined by the Object Management Group, primarily used for managing data interchange between lightweight devices and extensive networks of high-performance sensors. In industries like air traffic control, smart grid management, transportation, and healthcare services, DDS is employed for high-quality multicasting, operating over both UDP and TCP without requiring a broker [Kapoor and Kaur(2022)].

XMPP (Extensible Messaging and Presence Protocol) is an open XML technology for asynchronous real-time communication between two or more organizations, functioning as a client-server protocol that resembles SMTP and operates over TCP. XMPP offers robust security features, supporting SASL for authentication and TLS for data confidentiality. However, the lack of end-to-end encryption support makes the protocol vulnerable to various types of attacks [Kapoor and Kaur(2022)].

mDNS (multicast Domain Name System) is a zero-configuration service discovery protocol, extensively used for service discovery and name resolution on local connections, particularly in small networks without a local name server. When combined with DNS-based service discovery (DNS-SD), mDNS offers the flexibility needed for environments to automatically integrate new devices and perform DNS-like operations without requiring a traditional DNS server [Kapoor and Kaur(2022)].

SSDP (Simple Service Discovery Protocol) is an open protocol designed for advertising and discovering services, as well as presenting service information. Commonly utilized in home and small business environments, SSDP forms an integral part of the UPnP architecture, facilitating seamless operation of plug-and-play devices without requiring manual setup. As this protocol plays a significant role in IoT device functionality, users must remain vigilant about potential safety risks associated with device ownership and usage [Kapoor and Kaur(2022)].

OPC (Open Platform Communications) is an interoperability standard designed to facilitate the exchange of data in industrial automation, ensuring seamless information flow between devices from multiple vendors. The OPC Foundation is responsible for developing and maintaining this platform-independent standard. It was first developed in 1996 to translate PLC specific protocols (such as Modbus, Profibus, etc.) into a standardized interface allowing HMI/SCADA systems to interface with a "middleman" who would convert generic-OPC read/write requests into device-specific requests and vice-versa. The standard defines the interface between clients and servers, including access to real-time data, monitoring of alarms and events, and access to historical data. Initially, the standard was restricted to the Windows operating system, but the OPC UA specifications were developed to address new challenges in security and data modeling in manufacturing systems [Mahnke et al.(2009)].

OPC-UA, or Unified Architecture, was released in 2008 and is an integration of the individual OPC Classic specifications into a single, extensible multi-layered, service-oriented architecture. It provides platform independence and compatibility with a wide range of hardware platforms and operating systems, ensuring interoperability across the entire enterprise. OPC-UA is functionally equivalent to OPC Classic but offers enhanced capabilities such as [Mahnke et al.(2009)], [Foundation(2023)]:

- Discovery of OPC servers: OPC-UA enables automatic detection of available OPC servers, simplifying the process of connecting to various devices and systems.
- Hierarchical address space: OPC-UA features a structured address space with access mechanisms to information models, including a look-up mechanism and on-demand read/write data access.
- Subscriptions and event notifications: OPC-UA allows clients to subscribe to data changes and events, enabling real-time updates and efficient communication between devices.
- Server methods execution: OPC-UA permits clients to execute server methods, allowing for greater interaction and control between client applications and the server.
- Enhanced security features: OPC-UA addresses security concerns by providing a suite of controls, including transport protocols, session encryption, message signing, sequenced packets, authentication (X509 certificates), user control, and auditing.

OPC-UA supports both service-oriented and publish-subscribe communication models. In the service-oriented client-server model, the service provider processes the received requests, and sends the results back with the response. In the publish-subscribe model, OPC-UA offers a mechanism for data and event notification optimized for many-to-many configurations, where publishers send messages to a Message Oriented Middleware, and subscribers' express interest in specific types of data. Subscribers will process messages that contain their desired data, without needing to know the source [Mahnke et al.(2009)], [Foundation(2023)].

The multi-layered architecture of OPC-UA ensures a future-proof framework that allows for the integration of innovative technologies and methodologies while maintaining backwards compatibility with existing products. This makes OPC-UA an ideal choice for organizations looking to implement a robust, secure, and flexible communication standard for industrial automation and control systems [Mahnke et al.(2009)], [Foundation(2023)].

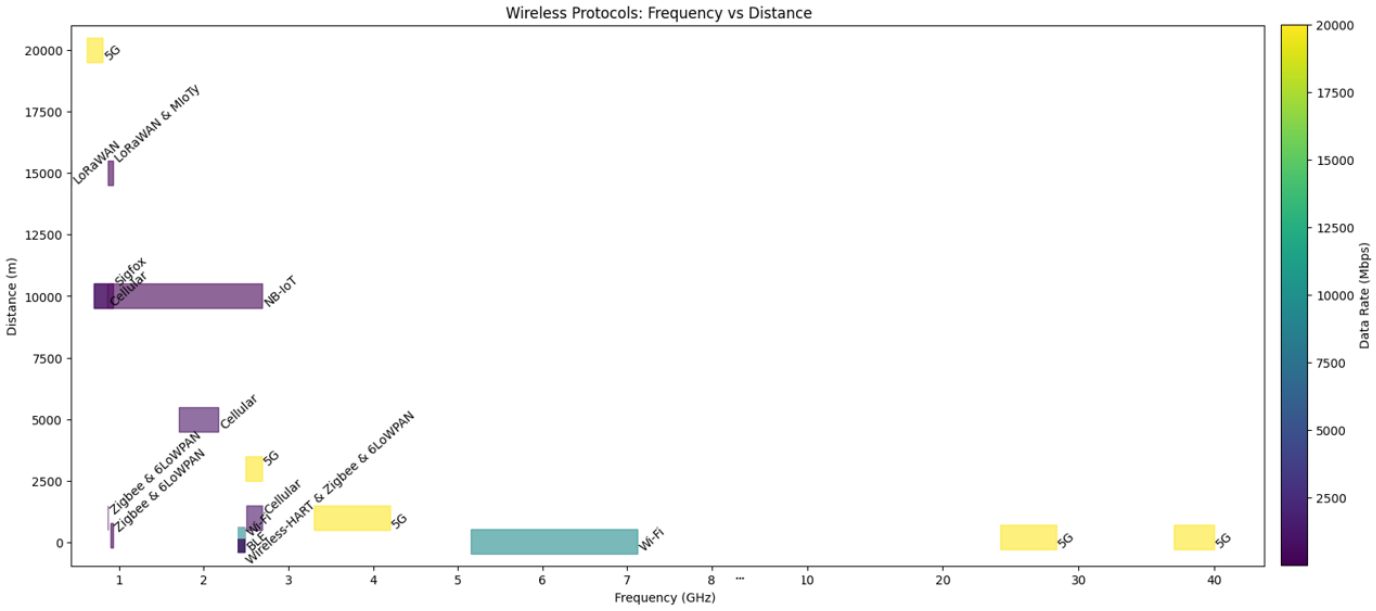

Fig. 4. Wireless protocols frequency vs distance.

V. IoT Wireless Physical and Link Layer Protocols

In this section, we discuss common wireless protocols for industrial edge communications. We carefully analyzed and clustered similar protocols by frequency range, coverage distance and data rate and provided a inclusive chart in Fig. 4. This chart can help identifying the potential unwanted interference, as well as facilitating decision making in choosing a protocol that is more suitable for our requirements.

In the following, protocols in this chart, which include IEEE802.15.4, Wi-Fi, Bluetooth, LPWAN and Cellular networks, are discussed in more details.

IEEE802.15.4 defines the standard for low-rate wireless personal area networks. It is used for a wide variety of protocols such as WirelessHART and Zigbee.

- **Wireless-HART** is a wireless communication protocol designed for industrial process automation. Introduced almost two decades ago, it has replaced Modbus in many industries and is estimated to have over 25 million field devices installed worldwide. It has a data rate of 250kbps and a typical distance range of 50-100m. With clear line of sight, the range can extend up to 250m. The protocol has two stacks for wireless operation. One is using the wireless-HART communication protocol for both the physical and datalink layers, operates in the 2.4 GHz ISM band and allows for reliable and secure wireless communication between sensors, actuators, and control systems. The other is based on IEEE 802.15.4 and provides Time Scheduled Channel Hopping (TSCH) at the data link layer, and self-organizing, mesh network at the network layer, to ensure reliable communication in harsh industrial environments. Both versions of the protocol provide auto-segmentation at the transport layer. Wireless-HART offers advanced features like multi-hop communication, encryption, and device diagnostics, making it a popular choice for process control and monitoring applications in industries [Kinney(2023)], [Bayou(2018)]. In Fig. 1, the HART protocol is shown which can be implemented in multiple ways:
  1) HART-IP can utilize Ethernet at the Physical and Link Layers, IP at the Network layer, and UDP or TCP at the Transport Layer; It can reach 1.2 kbps data rate and theoretically have the communication limit of 3km, which is dependent of the cable capacity.
  2) HART can be implemented with WirelessHART at the Physical and Link Layers, which represent simultaneous analog and digital signaling for the Physical Layer, a token passing controller/worker protocol for Link Layer. In this case it has a specific proprietary protocol for the Transport Layer that performs auto segmented transfers and a specific proprietary Application Layer, which is command oriented;
  3) HART can employ IEEE 802.15.4 at the Physical Layer on the 2.4 GHz frequency, with Time Synchronized Channel Hopping (TSCH) at the Link Layer, redundant paths mesh for the Network Layer and its proprietary protocol for both Transport and Application Layers.
- **Zigbee** is a variant of IEEE802.15.4, which is mainly used in home automation. It has low power consumption and can transmit over 330-1000 ft (100-300 m) in theory (30-330 ft [10-100 m] in practice with line of sight). Zigbee can transmit over a longer range using a mesh network of nearby Zigbee devices and supports 65,000 nodes using 16 RF channels in the 2.4 GHz band using DSSS (Direct Sequence Spread Spectrum) modulation and maximum data rate of 250 kbps. The Connectivity Standards Alliance manages Zigbee [Lennvall

et al.(2008)], [Alliance(2023a)].

Wi-Fi (Wireless Fidelity), originally designed as wireless Ethernet, provides high-speed Internet and network connections between devices using radio waves. It operates in the 2.4 GHz and/or 5 GHz frequency bands and uses a standard protocol known as IEEE 802.11. Wi-Fi operates in Mac and Physical Layer (see Fig. 1), provides carrier-sense multiple access with collision avoidance, and supports many TCP/IP compatible applications. Wi-Fi has multiple generations (802.11b/a/g/n/ac/ax/be), each increasing data rates by using different encodings [Links(2022)], [Shuka(2023)], which is briefly explained below:

- **Wi-Fi 1 (802.11b)** was the first widely adopted version of Wi-Fi and provided a maximum data rate of 11 Mbps and distance range of up to 35m indoor and 150m outdoor. It uses Direct Sequence Spread Spectrum (DSSS) modulation. It uses the 2.4 GHz frequency band and supports WEP encryption, which is now considered insecure and vulnerable to attacks [Links(2022)], [Shuka(2023)].
- **Wi-Fi 2 (802.11a)** uses the 5 GHz frequency band and provides a maximum data rate of 54 Mbps and distance range of up to 35m indoor and 150m outdoor. It uses Orthogonal Frequency Division Multiplexing (OFDM) Modulation which continued to be used in later versions of Wi-Fi along with other modulations. It supports WPA and WPA2 encryption, which are considered more secure than WEP [Links(2022)], [Shuka(2023)].
- **Wi-Fi 3 (802.11g)** uses the 2.4 GHz frequency band, uses OFDM modulation and provides a maximum data rate of 54 Mbps and distance range of up to 40m indoor and 150m outdoor. It supports WPA and WPA2 encryption and is backward compatible with Wi-Fi 1 devices [Links(2022)], [Shuka(2023)].
- **Wi-Fi 4 (802.11n)** uses both the 2.4 GHz and 5 GHz frequency bands and provides a maximum data rate of 600 Mbps and distance range of up to 70m indoor and 250m outdoor. It supports WPA and WPA2 encryption and introduced the use of MIMO (Multiple-Input Multiple-Output) technology to improve performance and range [Links(2022)], [Shuka(2023)].
- **Wi-Fi 5 (802.11ac)** uses the 5 GHz frequency band and provides a maximum data rate of up to 6.9 Gbps and distance range of up to 70m indoor and 250m outdoor. It supports WPA3 encryption, which is the latest and most secure encryption standard for Wi-Fi [Links(2022)], [Shuka(2023)].
- **Wi-Fi 6 (802.11ax)** provides a maximum data rate of up to 9.6 Gbps and distance range of up to 70m indoor and 250m outdoor. It uses both the 2.4 GHz and 5 GHz frequency bands and supports WPA3 encryption. It also introduces several new features, including 1024-QAM (Quadrature Amplitude Modulation), MU-MIMO (Multi-User Multiple-Input Multiple-Output) and OFDMA (Orthogonal Frequency Division Multiple Access) to improve performance in crowded environments [Links(2022)], [Shuka(2023)].
- **Wi-Fi 7 (802.11be)** is the next generation Wi-Fi that is under development and is expected to operate in the 6GHz frequency band. It is expected to offer faster speeds, higher capacity, and lower latency [Alliance(2024b)].

To protect against unauthorized access, Wi-Fi networks can be secured using encryption and authentication mechanisms such as WEP (RC4) and WPA2 (AES). With its ubiquitous presence in homes, businesses, and public spaces, Wi-Fi is used for a wide range of applications including web browsing, streaming media, VoIP, and IoT connectivity [Pahlavan and Krishnamurthy(2009)], [Pahlavan and Krishnamurthy(2013)].

Bluetooth (IEEE 802.15.1) is a full stack wireless controller/worker communication protocol that enables short-range data exchange (up to 330 ft [100 m] in theory) between up to 8 devices (one controller, 7 worker) at a time. It operates in the 2.4 GHz to 2.483 GHz ISM band, with 9 RF channels and a 1-3 Mbps data rate. Bluetooth uses frequency-hopping spread spectrum (FHSS) modulation to avoid interference, providing reliable and secure communication between devices. Within the stated range depending on the version and class, Bluetooth supports various profiles such as audio, data transfer, and human interface devices (HID). It is a popular choice for wireless headphones, keyboards, and other peripherals, as well as IoT devices [Bluetooth(2023)].

- **BLE**, or Bluetooth Low Energy, is a variation of Bluetooth that operates in the same 2.4 GHz band, but with lower power consumption and shorter range. It has a maximum data rate of 2 Mbps. Unlike Bluetooth, which only supports point-to-point communication, BLE allows for point-to-point, broadcast, and mesh communication topologies. BLE uses 128-bit AES encryption to provide secure communication between devices [Bluetooth(2023)]. Bluetooth is a full-stack protocol, offering a complete set of communication layers for seamless integration, as can be seen in Fig. 1.

LPWAN or Low Power Wide Area Networking, is a wireless wide area network that uses low bandwidth and low power consumption to send low-rate data over long distances. LPWANs are often battery-powered and designed for use in applications where traditional cellular or Wi-Fi networks are not feasible due to their high-power requirements. Examples of LPWAN technologies include LoRaWAN, Sigfox, Mioty, 6LowPAN and NB-IoT [Henke(2023)].

- **LoRaWAN** is a wireless communication protocol designed for low-power, wide-area networks (LPWANs). With an estimated 30 ms airtime for a 10-byte payload per km, it uses chirp spread spectrum modulation to provide long-range communication with low power consumption, making it ideal for Internet of Things (IoT) devices. Due to its low power and wide range communication capabilities, LoRaWAN is a popular choice for IoT applications in industries such as smart homes, agriculture, smart cities, warehouse monitoring, and logistics. As shown in Fig. 1, LoRa is the name used for the Physical Layer of the protocol and LoRaWAN is used for the Link Layer. LoRa operates on free, unlicensed frequency bands, typically using sub-GHz frequencies.

The frequency band is different based on the geographical location, e.g., in the US it is 915 MHz (902-928 MHz) and 868 MHz (863–870 MHz) in Europe. Depending on modulation and frequency, LoRa can provide up to 250 kbps data rate over long distance of 5 km in urban area and 15 km in rural area. LoRaWAN supports bi-directional communication, secure data transmission, and network scalability, as well as remote device management, firmware updates, and over-the-air activation. It also uses AES 128-bit encryption to ensure secure communication between devices. LoRaWAN can be integrated with MQTT [Network(2023)], [Alliance(2023b)].

- **NB-IoT**, or Narrowband Internet of Things, is a cellular radio access technology developed by the 3rd Generation Partnership Project (3GPP). It operates on licensed spectrum and is designed for applications that require frequent communication, wide coverage, deep indoor penetration, low cost, and long battery life. It can operate on both 4G and 5G cellular networks. NB-IoT uses OFDM modulation and 256-bit 3GPP encryption to achieve high connection density on a narrowband of 200 kHz. It is suitable for both commercial and consumer-based applications. It can reach the data rate of 30 kbps and distance of 15 km. As shown in Fig. 1, The CoAP protocol is recommended to run on top of NB-IoT, specifically LwM2M over CoAP [Larmo et al.(2018)]. HTTP and MQTT are not recommended to be used with NB-IoT as they are connection-oriented and can decrease battery life [AWS(2023)], [Abdelmoumen(2019)].
- **MIoTy** is a LPWAN protocol supported by the mioty alliance and Fraunhofer and is used for monitoring devices when high capacity, high density, mobility, long distance, and low power usage. It is working in license free spectrum (863-928 MHZ) and can provide up to 1.5 kbps data rate over long distance of 5 km in urban area and 15 km in rural area and data rate of up to 512 pbs. It splits data telegram into sub packets, applies error correction code and sends them in a predefined time and frequency band using two channels for uplink and downlink [Alliance(2024a)].
- **Sigfox** is a full stack (see Fig. 1) proprietary protocol owned by UnaBiz which works in free spectrum (862-928 MHz) used for low power wide area network communication. It uses ultra narrow band which is a wide-reaching signal that passes through objects. Sigfox can cover the range of up to 10 km in urban area and 40 km in rural area and has the data rate of 100 bps or 600 bps depending on the region [unabiz(2024)], [Abdelmoumen(2019)].
- **6LowPAN** is defined by IETF and stands for IPv6 Over low power WPAN, typically operates at frequencies below 1 GHz or in the 2.4 GHz frequency band. It is a mesh network where each node has an IPv6 address so that each low power device can connect to the Internet directly. It has the data rate of up to 250 kbps and coverage of up to 100 m. Physical and Mac Layers are designed for one hop neighbor transmission. It has a network encapsulation that supports neighbor discovery (ND), header compression, optimization, and selective fragment recovery to allow IPv6 work over IEEE 802.15.4 [unabiz(2024)].

Cellular Networks have evolved significantly over the past few decades, and each generation has brought new capabilities and features to users [Bhandari et al.(2017)], [Vora(2015)].

- **First generation (1G)** of cellular networks was analog and used Frequency Division Multiple Access (FDMA) technology. Security in 1G was non-existent, as the networks were not designed to handle data, and encryption mechanisms were not yet available [Bhandari et al.(2017)], [Vora(2015)].
- **Second generation (2G)** introduced digital signals and used Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) technologies to increase network capacity. It has 64 kbps data rate. 2G networks provided basic encryption mechanisms such as A5/1 and A5/2, but these were eventually found to be vulnerable to attacks. GSM (Global System for Mobile Communications) was one of the most frequent 2G technologies [Bhandari et al.(2017)], [Vora(2015)].
- **Third generation (3G)** provided faster data speeds and introduced new security features such as Universal SIM (USIM) cards, mutual authentication, and improved encryption algorithms such as KASUMI. It has 8 Mbps data rate. [Bhandari et al.(2017)], [Vora(2015)].
- **Fourth generation (4G)** networks offered even faster data speeds and improved network reliability, along with more advanced security features such as Advanced Encryption Standard (AES) and Internet Protocol Security (IPsec). LTE (Long-Term Evolution) is one of the most widely used 4G technologies. It is based on a packet-switched network architecture, which allows for more efficient use of network resources and faster data transfer speeds. LTE can provide data transfer rates of up to 300 Mbps for download and up to 75 Mbps for upload, although the actual data transfer rates may vary depending on the network coverage, device, and network congestion. LTE is widely used by mobile network operators around the world and is the backbone of many mobile data plans [Bhandari et al.(2017)], [Vora(2015)].
- **Fifth generation (5G)** is the current generation and offers even faster speeds, reduced latency, and improved connectivity for IoT devices. It can reach to the data rate of up to 10 Gbps. 5G also includes new security features such as 5G-AKA, a more secure version of the Authentication and Key Agreement (AKA) protocol used in 3G and 4G networks, as well as new encryption algorithms such as ZUC and SNOW 3G. However, as with any new technology, there are concerns about potential security vulnerabilities, and ongoing security updates will be required to ensure that 5G networks remain secure [Bhandari et al.(2017)], [Vora(2015)].

VI. ICS Protocols and Standards

This section explains the most commonly used protocols for industrial control systems. Fig. 1 shows the networking layer of these protocols and their compatibility with other layers' protocols.

Fieldbus is an IEC standard that enables real-time distribution control of low-level industrial field equipment, including sensors, switches, and actuators (such as valves and lamps). It supports ring topology with a maximum length of (6,200 ft) 1900 m and operate at 31.25 kbps. Fieldbus uses the serial line of un/shielded twisted pairs as media. Modbus, Profibus, Device Net, and Foundation Fieldbus are some of its popular protocols [Hahn et al.(2010)].

Modbus was originally introduced by Modicon 1979 and now owned by Schneider Electric. It is a request-response, controller/worker data communication protocol that has been widely used for monitoring and controlling PLCs. It uses port 502, the data rate is 9.6 kbps and 19.2 kbps, and range less than 1,000 ft (300 m). It uses a serial line of un/shielded twisted pairs as media. Modbus has three different stack presentations as shown in Fig. 1 [Hahn et al.(2010)], [Byres et al.(2004)].

- Modbus RTU works with Serial line RS-232 (standard for serial communication transmission of data) or RS-485 (standard for serial communication transmission of data over long distances).
- Modbus Plus uses High-level Data Link Control (**HDLC**) which provides error checking for reliable communication.
- Modbus TCP is compatible with Ethernet networks. Profibus developed in 1989 by BMBF and Siemens and is used for monitoring and controlling process automation. The data rate is 9.6 kbps and 31.25 kbps to 12Mbps, and range is 4,000 ft (1200 m). It uses serial line of un/shielded twisted pairs as media [Hahn et al.(2010)], [Neumann and Poschmann(2005)].

PROFINET was introduced in 2003 and is used for exchanging data between controllers (PLCs, DCSs, PACs, etc.) and devices to satisfy the requirements of automated technology. It uses Ethernet to collect the data and control the equipment. The range is 330 ft (100 m) and can operate on the speed of 100 Mbps. It is the most well adopted industrial Ethernet and it is compatible with TCP/UDP, IP and Ethernet IEEE802.3 [Neumann and Poschmann(2005)], [Bowne(2023)]. As shown in Fig. 1, Profinet can either work directly over EtherCAT or can use UDP or TCP and IP to work over EtherCAT and Ethernet.

DNP3, also known as IEEE std 1815, is used between components of process automation systems mostly in electric power and water companies. It is a TCP/UDP, IP based communication and some recent applications have implemented it over Ethernet. DNP3 is used in SCADA and remote monitoring systems [Staff(2023)]. DNP3 is compatible with both TCP and UDP, and IP over Ethernet, as shown in Fig. 1.

EtherNet/IP is an industrial application protocol that was developed by Rockwell Automation in the late 1990s for industrial factories and it is managed by ODVA (Open Device Net Vendors Association) [Pimentel and Schneider(2016)]. The data rate can be as high as 100 Mbps and the maximum cable length between nodes is 100 m. It operates under the common industrial protocol (**CIP**), an open application layer protocol and, as shown in Fig. 1, it is compatible with TCP/UDP, IP and Ethernet [Pimentel and Schneider(2016)].

IEC 60870-5-104, IEC 61850, and IEC 62351 are all communication protocols used in SCADA systems working over TCP/IP as shown in Fig. 1.

- IEC 60870-5-104 is used for real-time data and control commands over LAN and WAN and has a client server architecture. It is compatible with TCP/IP and has an additional application protocol control information layer (APCI) in its application layer [Egger et al.(2020)].
- IEC 61850 exchanges real-time data, control commands, and status information over Ethernet networks. IEC 61850 uses three approaches: i) the client server architecture using TCP/IP, ii) the Goose approach, which is mostly used for multicast and publishes the information of time sensitive data with high priority via Ethernet, and iii) sampled value. IEC 61850 uses Ethernet and is commonly applied to the merging of analog values in power utility applications [Castro and Zaninelli(2019)], [Hussain et al.(2019)].
- IEC62351 provides security mechanisms for IEC61850 [Hussain et al.(2019)].

S7Comm is a proprietary protocol developed by Siemens in 1994, used for communication between Siemens PLCs, as well as PLC and other control systems elements such as DCS and SCADA. It operates using ISO-on-TCP (RFC 1006 or COTP) and identifies the communication type and position of the PLC (slot and rack). The S7-400 version uses COTP without TCP/IP [SIEMENS(2023)].

HART protocol was developed by Rosemount Inc. (a subsidiary of Emerson Electric Company). It is used for connecting analog and digital sensors and actuators in process control. It can operate over Ethernet/IP with both TCP and UDP, with a data rate of 1200 and 3600 bps. The range of HART is less than 10,000 ft (3000 m). HART also has two versions called HART-IP and Wireless Hart. HART-IP works over both TCP and UDP, which operate on top of IP and Ethernet [Hahn et al.(2010)], [Lennvall et al.(2008)].

IO-Link is an industrial protocol defined by IEC 61131-9. It is used over short distances (20 m) and for wired point-to-point communication for connecting devices such as sensors and actuators to master (e.g., PLC) [ISA(2024)]. As shown in Fig. 1, it is a full stack protocol. It has 3 settings for baud rate 4.8k, 38.4k and 230.4k.

EtherCAT is an Ethernet based fieldbus standardized as IEC61158 and is a controller/worker protocol used for real-time industrial communications with high-speed and low latency. It can transfer data at 100 Mbps over distances of up to 100 m, although using optical fiber can increase the distance. It is compatible with many application protocols such as CANopen, Sercos, Modbus and Profinet. TCP/IP is an optional layer for non-fieldbus application protocols such as HTTP and FTP. There is no requirement for a switch if only EtherCAT is used in the network. EtherCAT Frames are basically the same as EtherNet IEEE 802.3, but they are optimized for increase bandwidth and short cycle data [Rostan et al.(2024)].

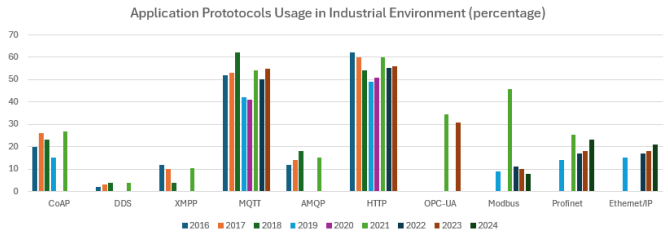

Fig. 5. Application protocols usage in industries

VII. Analysis of Protocols: Statistics, Vulnerabilities, and Industrial Trends

In this section, we analyze the industry and market trends, security vulnerabilities, and weaknesses associated with various protocols across IT, ICS, IoT, and Wireless communication sectors. Leveraging data from the Common Vulnerabilities and Exposures (CVE) database and the Common Weakness Enumerations (CWE) list from NIST [National Institute of Standards and Technology(2023)] and the MITRE CVE list [MITRE Corporation(2023)], we gain a deeper understanding of the security landscape. CVE provides a list of publicly disclosed cybersecurity vulnerabilities, such as CVE-2021-34527 (PrintNightmare vulnerability). CWE categorizes the types of weaknesses that can lead to these vulnerabilities, such as CWE-89 (SQL Injection). The severity of these vulnerabilities is assessed using the Common Vulnerability Scoring System (CVSS). Fig. 5 [1] illustrates the usage of different application protocols in industries, highlighting the sectors where these protocols are most commonly deployed [Arista Networks(2022)], [Aloufi and Alhazmi(2020)], [Bayılmış et al.(2022)], [world(2022)]. Understanding the application and market trends of these protocols is crucial for a comprehensive security analysis. Increased adoption of a particular protocol often leads to a higher number of reported CVEs. This increase may not necessarily indicate inherent weaknesses in the protocol itself, but rather stem from its growing usage, which can result in more faulty implementations and attract greater attention from attackers.

A. IT Protocols

IT protocols form the full stack backbone of modern digital communication. Fig. 6 and 7 depict the CVEs and CWEs for IT protocols of differetnt layers including Ethernet, IP, TCP, UDP, SSL, TLS, SOAP, REST, XML, SMTP, and HTTP. SSL and HTTP show a high frequency of severe vulnerabilities (CVSS scores 7-10), reflecting security concerns and underscoring the importance of securing web and communication protocols. The significant increase in the number of CVEs for SSL around 2014 can be attributed to the Heartbleed and Poodle attacks on OpenSSL (covering both SSL and the flawed implementation of TLS as well as the usage of older TLS versions). These incidents highlighted the critical need for timely security updates and adherence to the latest standards.

[1]Finding trustworthy source of information on protocol usages were a challenging task. No bars for certain years were due to lack of publicly available information.

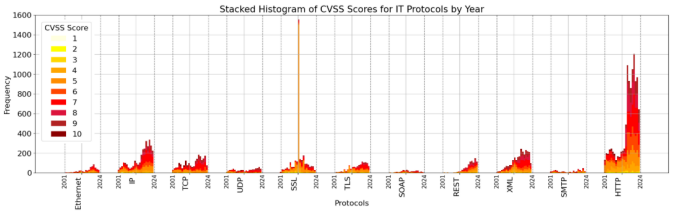

Fig. 6. Vulnerabilities (CVEs) per IT protocol over years

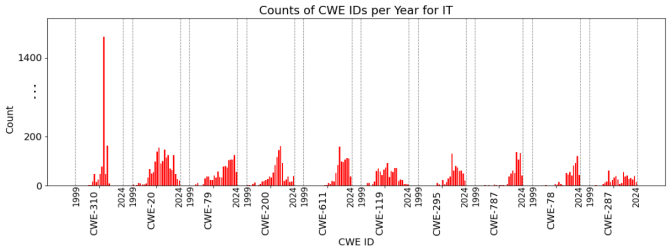

Fig. 7. Weaknesses (CWEs) per IT protocol over years

Other layer protocols, such as TCP and IP, also exhibit notable vulnerabilities in the network backbone. Fig. 7 demonstrates that cryptographic issues (CWE-310) are a significant weakness in IT protocols and mostly in the implementation of encryption and key management practices. Addressing cross-site scripting (CWE-79), information exposure (CWE-200), and buffer overflow (CWE-119) vulnerabilities will further enhance IT security.

B. ICS Protocols

Industrial Control Systems (ICS) protocols are critical for managing and controlling industrial processes. The growth of Industrial Ethernet in the industry, as reported by HMS market analyses [Olson(2019)], [Nalin(2021)], [HMS(2023)], indicates a trend towards incorporating TCP/IP into industrial protocol stacks. This shift enhances compatibility with TLS, thereby making it more feasible to implement stronger security measures. Profinet and Ethernet/IP demonstrate steady usage, highlighting their reliability and prevalence in industrial networks. Fig. 8 and 9 show the CVEs and CWEs for ICS protocols including HART, Modbus, Profinet, HDLC, RS-485, RS232, Serial Line, CIP, DNP3, S7comm, IEC 60870-5-1-4, IEC 61850, and IEC 62351. Modbus and DNP3 show a higher frequency of severe vulnerabilities (CVSS scores 7-10), indicating significant security concerns in their older versions. This highlights the critical need for improved security measures, such as instead of using Modbus with RTU build it with TCP/IP stack and add TLS or in DNP, add DNP3-SA (Secure Authentication) between DNP3 application and DNP3 transportation layer. Profinet also has notable vulnerabilities but less severe compared to Modbus and DNP3, suggesting ongoing but manageable security risks in this protocol. The CWE chart demonstrates that improper input validation (CWE-20) is a major security weakness in ICS protocols, necessitating better validation mechanisms. Addressing buffer overflow and authentication issues will further enhance the security of ICS

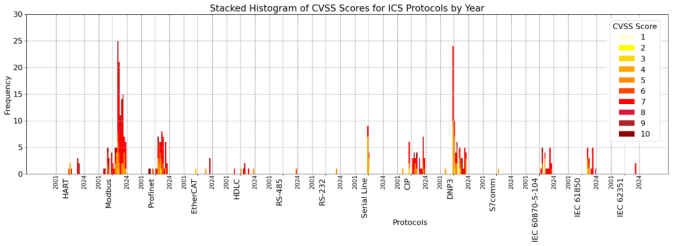

Fig. 8. Vulnerabilities (CVEs) per ICS protocol over years

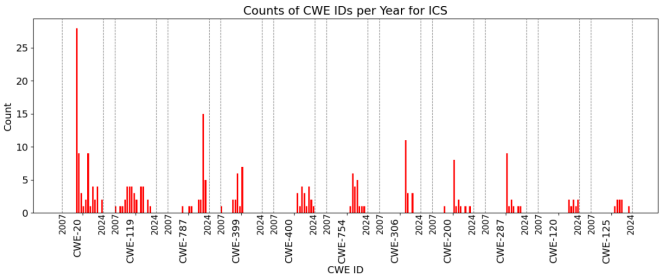

Fig. 9. Weaknesses (CWEs) per ICS protocol over years

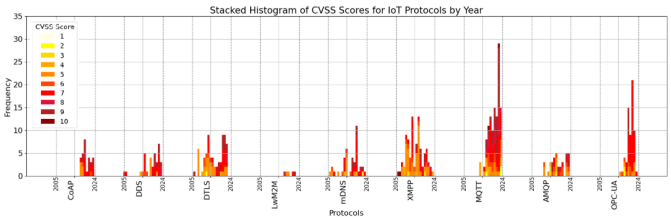

Fig. 10. Vulnerabilities (CVEs) per IoT protocol over years

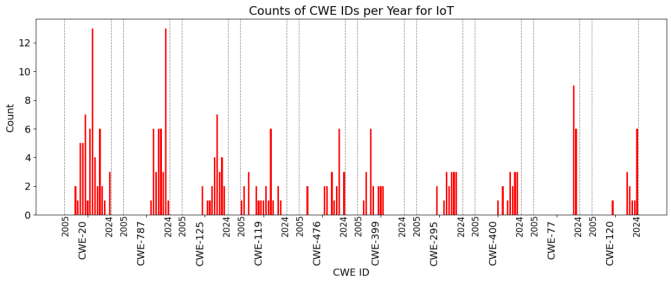

Fig. 11. Weaknesses (CWEs) per IoT protocol over years

systems. Timely security updates are crucial for ICS protocols considering their critical environments.

C. IoT Protocols

The Internet of Things (IoT) is expanding rapidly as depicted in Fig. 5, with projections indicating that nearly half of IoT applications will incorporate AI by 2027 [Lueth(2023)]. MQTT and HTTP protocols have consistently high usage, indicating their importance in industrial applications. MQTT's popularity is likely due to its lightweight nature, suitable for IoT applications. OPC-UA shows significant growth, reflecting its increasing adoption in industrial automation and control systems, indicates a trend towards more robust, secure communication standards in industrial automation. Fig.10 and 11 show the CVEs and CWEs for IoT application protocols including CoAP, DDS, DTLS, LwM2M, mDNS, XMPP, MQTT, AMQP, and OPC-UA. As IoT protocols see higher adoption, the peak of CVEs is more pronounced in recent years compared to ICS and IT protocols. The high severity of vulnerabilities in recent years in MQTT and OPC-UA highlights the need for enhanced security frameworks in IoT applications. This necessitates the use of the latest version, such as MQTT5, or securing communication by using TLS with MQTT brokers like HiveMQ. Addressing Man-in-the-Middle (MITM) vulnerabilities, which can lead to eavesdropping and message tampering in DTLS and CoAP, enhances their security. The CWE chart reveals the prevalence of input validation and memory management issues (CWE-20, CWE-787, CWE-125, CWE-119), indicating a critical need for robust error handling and validation mechanisms in IoT protocols. Improving data protection and secure communication practices (CWE-200, CWE-295) will further enhance IoT security.

The transition to AIoT is accelerating, with only 7% of IoT applications being AI-infused in 2022, but nearly half expected to incorporate AI by 2027 [Lueth(2023)]. The transition to AIoT (Artificial Intelligence of Things) introduces new security challenges, making it crucial to address vulnerabilities early in the development cycle to ensure the safe deployment of IoT devices.

D. Wireless Protocols

Wireless link and physical layer protocols are becoming increasingly prevalent in both industrial and consumer applications. Fig. 12 provides insights into the usage of wireless protocols in industry on the left [Oza(2019)] and the global market share of wireless protocols on the right [Market Research Future(2024)], [Wood(2024)]. The steady usage of Wi-Fi and IEEE 802.15.4 underscores their importance in industrial wireless communications and their compatibility with more upper layer protocols. The growth in BLE and LPWAN usage suggests a trend toward energy-efficient and long-range communication solutions. Fig. 13 and 14 show the security vulnerabilities of wireless protocols such as Wi-Fi, LoRaWAN, Cellular, BLE, and IEEE 802.15.4 (including Zigbee, WirelessHart, 6LoWPAN, and others). The data highlights that the growing adoption of wireless protocols brings with it an increasing number of security challenges and the need for robust security measures becomes even more critical.

Wi-Fi frequently exhibits severe vulnerabilities, as indicated by high CVSS scores (7-10). This is not surprising given its widespread use, and it's compatibility with many different protocols and applications, but it also highlights significant security challenges. Initial weaknesses in WEP, such as the short Initialization Vector (IV) length, were addressed in WEP2 by extending both the IV and key lengths to 128 bits. However, it became clear that the fundamental flaws in the WEP algorithm went beyond just the IV and key lengths, necessitating a more comprehensive solution. Other protocols such as BLE and Zigbee also exhibit notable vulnerabilities but are less severe than Wi-Fi. Memory management issues

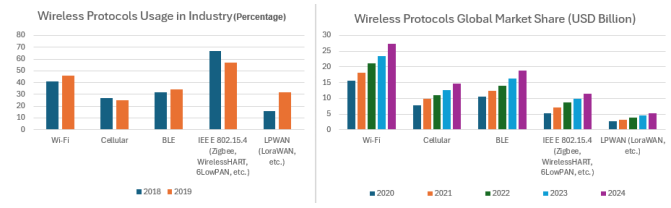

Fig. 12. Wireless protocols usage

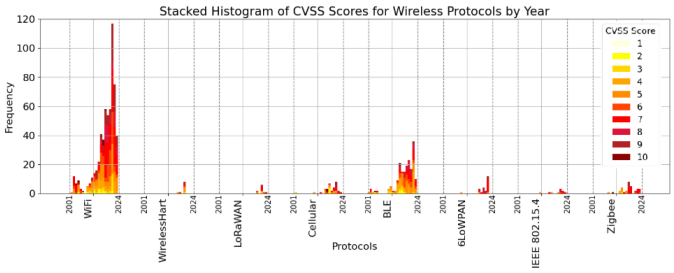

Fig. 13. Vulnerabilities (CVEs) per Wireless protocol over years

(CWE-787, CWE-125) are significant weaknesses in wireless protocols, necessitating better error handling and validation mechanisms. Improving input validation (CWE-20) and data protection practices (CWE-200) will further enhance wireless security.

These application statistics, combined with the security vulnerability data, provide a comprehensive overview of the current state and future trends in protocol usage and security. This holistic view helps stakeholders make informed decisions about which protocols to implement and how to prioritize security investments. Key points highlighted by the data include:

- Evolving Threat Landscape: The increase in CVEs and CWEs over time across IT, IoT, and Wireless protocols underscores the evolving nature of security threats accompanying the adoption of these communications. The trend in ICS is somewhat different, potentially indicating an increased awareness of security in industrial environments or a shift from legacy protocols to more modern TCP-based and IoT protocols, as confirmed by HMS market analysis. Understanding the protocol stack and its layers is essential in identifying where these threats can penetrate and how to fortify each layer against emerging vulnerabilities.

- Sector-Specific Vulnerabilities: Each sector (IT, ICS, IoT, Wireless) has its own unique vulnerabilities and weaknesses.

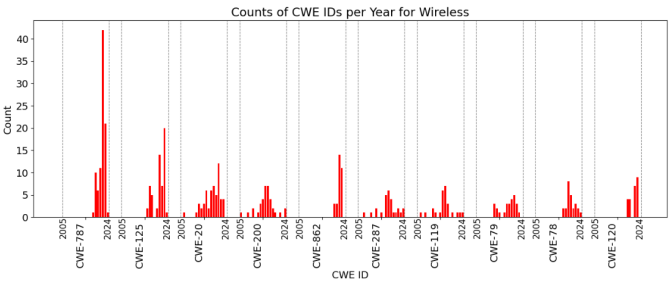

Fig. 14. Weaknesses (CWEs) per Wireless protocol over years

Understanding these sector-specific issues is essential for developing targeted security strategies. A comprehensive knowledge of the protocol stack is invaluable in identifying which overlapping protocols in the same layer across different sectors are most at risk.

- Impact of Major Vulnerabilities: Events like the Heartbleed and Poodle attacks significantly impact protocol security, leading to spikes in CVEs. Such incidents illustrate the importance of rapid response and mitigation strategies to address emerging threats effectively. Knowledge of the protocol stack can guide stakeholders in quickly identifying which layers are compromised and how best to respond.

- Growth and Adoption Trends: The increasing adoption of IoT and the growth of wireless networks in industrial environments highlight the need for forward-looking security measures that can adapt to new technologies and applications. Proactively addressing the security of AI in IoT before the widespread adoption of AIoT is crucial to prevent future security spikes. Understanding the protocol stack ensures that security measures are integrated at every layer, accommodating the complex interactions between different technologies.

By comparing the security profiles of different protocols, organizations can make informed decisions about which protocols with which stack layers to adopt based on their security needs and the specific threats they face. These charts collectively highlight the evolving threat landscape across various protocols and sectors. Common themes include the need for improved input validation, memory management, and cryptographic practices. Addressing these vulnerabilities will enhance the security and reliability of IT, ICS, IoT, and wireless protocols in industrial and other environments.

By understanding these vulnerabilities, assessing their severity, and analyzing trends, stakeholders can better protect their systems and data. This comprehensive approach to protocol security is essential for maintaining the integrity and reliability of modern communication networks. Continuous education, investment in security technologies, and adherence to best practices are paramount to mitigating risks and safeguarding critical infrastructure. Familiarity with the protocol stack and its layers not only aids in the immediate identification and resolution of security issues but also in the strategic planning of long-term security measures.

VIII. Discussion

The compatibility stack (Fig. 1) along with the frequency chart (Fig. 4) can be used across industries as two comprehensive tools that provides great insights into specifications of protocols. Compatibility stack enhances the interoperability of IIoT systems and boosts their performance across various industrial applications. It also aids in decision-making by aligning application requirements with protocol specifications. The frequency chart can help identifying the potential unwanted interference, as well as facilitating decision making in choosing a protocol that is more suitable for our requirements. In this section, we review a variety of use cases that can benefit from a clear understanding of the compatibility of IIoT protocols across different layers.

The primary reason for developing this classification was security. This protocol stack provides a deeper view into our network by identifying the protocols used across layers of network encapsulations. It can be used to study vulnerabilities and security issues associated with these protocols, allowing for greater focus on cybersecurity consulting, research, and policymaking to ensure the safety and protection of IIoT systems. By visualizing these interactions, system designers can identify vulnerable points where insecure protocols interact with more secure ones, making it easier to predict attack vectors and implement security measures. As a result, it can guide engineers to upgrade or implement encryption and authentication methods where required to make up for lack of security in any layer where required/ applicable. It also helps in designing a secure network architecture that meets security requirements.

The insight provided by this stack can also help identify potential failure issues. When an issue arises, it can help isolate the cause by understanding what is potentially causing the problem. It also helps increase reliability by incorporating redundancy and allocating redundant protocols for backup communication during fallbacks, thus improving overall reliability and uptime.

By understanding the compatibility and interaction of protocols, engineers can design systems optimized for performance, data rate, reachable distance, and security, choosing the most efficient combination of protocols for their application. For example, industries can select energy-efficient protocols across layers for battery-powered sensors or low-power devices to extend the lifetime of IoT devices without compromising functionality. In real-time or latency-sensitive applications, engineers can ensure that time-sensitive data flows smoothly across the network by selecting the proper protocol stack to improve response time. This stack can serve as a guide for integrating new devices and components without causing conflicts or interoperability issues. It also helps in the smoother transition from old protocols to new ones by understanding the impact of migration from one protocol to another across different layers. Additionally, it can guide purchasing decisions to ensure devices fit into existing networks and architectures seamlessly.

Ensuring compliance with widely accepted industry standards is another benefit of having a deep understanding of existing protocols and their specifications. The combination of compatible protocols across layers may meet certain requirements that would otherwise necessitate proprietary protocols, which increase the risk of security issues and incompatibility with other devices or future developments. It also helps avoid vendor lock-in and fosters a modular, flexible environment by integrating multi-vendor solutions and mixing and matching technologies based on protocol compatibility. If industries adhere to standard protocols, audits would be easier for regulatory bodies. Moreover, regulatory bodies familiar with this protocol compatibility stack can better aid companies by having a more insightful understanding of protocol vulnerabilities and compatibility.

The compatibility stack can also be used to identify gaps, providing opportunities to create new protocols that address these gaps and bridge existing incompatibilities across layers. It can inspire new services by leveraging protocol interactions and specifications, especially in emerging AI-driven IIoT edge computing or developing smart devices capable of switching between protocols based on requirements in a changing environment.

Analyzing historical CVE data for each protocol can help differentiate between vulnerabilities inherent to the protocol and those caused by improper implementation. This broader view can help make wiser choices when selecting, procuring, or developing a device or solution. Future research can build on this work to explore new protocols and their compatibility with the existing stack and monitoring their vulnerabilities.

IX. Conclusion

This paper presents a comprehensive review of Industrial Internet of Things (IIoT) standards and protocols, focusing on their compatibility with each other. Through an intensive research process, we analyzed the most frequently used protocols in IIoT and proposes a compatibility stack that can guide system designers and engineers in selecting the most appropriate communication protocols for their applications. This stack is the first of its kind and serves as a valuable resource for researchers, engineers, and practitioners in the field. The findings of the study can be used to advance IIoT technologies and their applications in modern industrial settings.

The compatibility stack enhances the interoperability of IIoT systems and improves their performance in various industrial applications. In this paper we used it to study vulnerability and security issues associated with these protocols, allowing for greater focus on cybersecurity consulting, research, and policymaking to ensure the safety and protection of IIoT systems. Future research can build on this work to explore new protocols and their compatibility with the existing stack.

Acknowledgment

We would like to thank FM's "Future of Industry, Cyber Research Team", especially Scott Bartlett, for their invaluable discussions and feedback.

References

[Abdelmoumen(2019)] R. Abdelmoumen. 2019. A Review of Link Layer Protocols for Internet of Things. *International Journal of Computer Applications* 182, 46 (2019).

[Abdullah and Ehsan(2014)] M. Abdullah and A. Ehsan. 2014. Routing protocols for wireless sensor networks: classifications and challenges. *Journal of Electronics and Communication Engineering Research* 2, 2 (2014), 05–15.

[Alliance(2023a)] Connectivity Standards Alliance. 2023a. Zigbee The Full-Stack Solution for All Smart Devices. Available: https://csa-iot.org/all-solutions/zigbee/2023.

[Alliance(2023b)] LoRa Alliance. 2023b. LoRa Alliance. Available: https://lora-alliance.org/2023.

[Alliance(2024a)] Mioty Alliance. 2024a. Stackforce Mioty Protocol Stack. Available: https://mioty-alliance.com/projects/stackforce-mioty-protocol-stack/.

[Alliance(2017)] O.M. Alliance. 2017. Lightweight Machine to Machine Technical Specification. Available: https://www.openmobilealliance.org/release/LightweightM2M/V1_0_2-20170208-A/OMA-TS-LightweightM2M-V1_0_2-20170208-A.pdf.

[Alliance(2024b)] Wi-Fi Alliance. 2024b. Wi-Fi Certified 7. Available: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-7.

[Aloufi and Alhazmi(2020)] Khalid Aloufi and Omar Alhazmi. 2020. Secure IoT Resources with Access Control over RESTful Web Services. 6 (01 2020). https://doi.org/10.5455/jjee.204-1581015531

[Arista Networks(2022)] Arista Networks. 2022. 10 Minutes in the Life of the Network. https://arista.my.site.com/AristaCommunity/s/article/10-Minutes-in-the-Life-of-the-Network#Comm_Kna_ka02I000000brV8QAI_5810

[AWS(2023)] AWS. 2023. Implementing LPWAN IoT Solutions on AWS Using NB-IoT and LTE-M. Available: https://docs.aws.amazon.com/whitepapers/latest/implementing-lpwan-solutions-with-aws/implementing-lpwan-iot-solutions-on-aws-using-nb-iot-and-lte-m.html2023.

[Baudoin et al.(2021)] C. Baudoin, E. Bournival, and E. Clauer. 2021. Global Industry Standards for Industrial IoT.

[Bayılmış et al.(2022)] Cüneyt Bayılmış, M Ali Ebleme, Ünal Çavuşoğlu, Kerem Küçük, and Abdullah Sevin. 2022. A survey on communication protocols and performance evaluations for Internet of Things. *Digital Communications and Networks* 8, 6 (2022), 1094–1104. https://www.sciencedirect.com/science/article/pii/S2352864822000347

[Bayou(2018)] L. Bayou. 2018. *Assessment and Enforcement of Wireless Sensor Network-Based SCADA Systems Security*. Ph. D. Dissertation. Ecole Nationale Supérieure Mines-Télécom Atlantique.

[Bhandari et al.(2017)] N. Bhandari, S. Devra, and K. Singh. 2017. Evolution of Cellular Network: From 1G to 5G. *International Journal of Engineering and Techniques* 3, 5 (2017).

[Bluetooth(2023)] Bluetooth. 2023. Bluetooth Wireless Technology. Available: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/2023.

[Bowne(2023)] M. Bowne. 2023. What is PROFINET? Available: https://us.profinet.com/profinet-explained/.

[Byres et al.(2004)] E.J. Byres, M. Franz, and D. Miller. 2004. The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. In *Citeseer*. 3–10.

[Castro and Zaninelli(2019)] A. Castro and D. Zaninelli. 2019. Introduction of Current Limiting Impedance for a Previously Solid Grounded Medium Voltage Distribution Network. In *IEEE*. 1–6.

[Cisco Systems(2023)] Inc. Cisco Systems. 2023. TCP/IP Overview. Available: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html.

[Egger et al.(2020)] M. Egger, G. Eibl, and D. Engel. 2020. Comparison of Approaches for Intrusion Detection in Substations Using the IEC 60870-5-104 Protocol. *Energy Informatics* 3 (2020), 1–17.

[Erwinski et al.(2023)] K. Erwinski, D. Karpinska, M. Kunz, M. Paprocki, and J. Czokow. 2023. An autonomous city-wide light pollution measurement network system using LoRa wireless communication. *Sensors* 23, 11 (2023), 5084.

[Foundation(2023)] OPC Foundation. 2023. The Industrial Interoperability Standard. Available: https://opcfoundation.org/about/opc-technologies/opc-ua.

[Friedl et al.(2014)] S. Friedl, A. Langley A. Popov, and E. Stephan. 2014. Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension.

[Ghayvat et al.(2014)] H. Ghayvat, A. Nag, NK. Suryadevara, SC. Mukhopadhyay, X. Gui, and J. Liu. 2014. Sharing research experiences of WSN based Smart Home. *International Journal on Smart Sensing and Intelligent Systems* 7, 4 (2014), 1997–2013.

[Gourley and Totty(2002)] D. Gourley and B. Totty. 2002. *HTTP: The Definitive Guide*. O'Reilly Media, Inc.

[Hahn et al.(2010)] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan, S. Sridhar, and M. Higdon. 2010. Development of the PowerCyber SCADA security testbed. In *CSIIRW '10: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*. 1–4.

[Harold and Means(2004)] E.R. Harold and W.S. Means. 2004. *XML in a Nutshell: A Desktop Quick Reference*. O'Reilly Media, Inc.

[Henke(2022)] C. Henke. 2022. A Comprehensive Guide to IoT Protocols. Available: https://www.emnify.com/iot-glossary/guide-iot-protocols.

[Henke(2023)] C. Henke. 2023. A Comprehensive Guide to IoT Protocols. Available: https://www.emnify.com/iot-glossary/guide-iot-protocols.

[Hirsch et al.(2007)] F. Hirsch, J. Kemp, and J. Ilkka. 2007. *Mobile Web Services: Architecture and Implementation*. John Wiley & Sons.

[HMS(2023)] HMS. 2023. *Continued growth for Industrial Ethernet and wireless networks*. https://www.hms-networks.com/news/news-details/21-05-2023-industrial-network-market-shares-2023

[Howie et al.(2004)] D. Howie, M. Ylianttila, E. Harjula, and J. Sauvola. 2004. State-of-the-art SIP for mobile application supernetworking. In *Proceedings of Nordic Radio Symposium, including Finnish Wireless Communications Workshop (NRS/FWCW 2004)*. Oulu, Finland.

[Hussain et al.(2019)] S.S. Hussain, T.S. Ustun, and A. Kalam. 2019. A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges. *IEEE Transactions on Industrial Informatics* 16, 9 (2019), 5643–5654.

[ISA(2024)] ISA. 2024. IO-Link Field Device Protocol Architecture. Available: https://www.isa.org/intech-home/2016/may-june/features/io-link-field-device-protocol-architecture.

[Kapoor and Kaur(2022)] M. Kapoor and P.J. Kaur. 2022. Analysis of Various Security Schemes of Internet of Things. In *Information and Communication Technology for Competitive Strategies (ICTCS 2021) Intelligent Strategies for ICT*. Springer, 163–171.

[Kinney(2023)] Pat Kinney. 2023. Overview of Mesh Networking over IEEE 802.15.4. Available: https://www.ieee802.org/1/files/public/docs2013/liaison-15-13-0493-01-0000-examples-of-mesh-networking-over-ieee-802-15-4-0913.pptx.

[Kurose and Ross(2010)] J. Kurose and K. Ross. 2010. *Computer Networks: A Top Down Approach Featuring the Internet*. Pearson Addison Wesley.

[Larmo et al.(2018)] A. Larmo, A. Ratilainen, and J. Saarinen. 2018. Impact of CoAP and MQTT on NB-IoT system performance. *Sensors* 19, 1 (2018), 7.

[Lennvall et al.(2008)] T. Lennvall, S. Svensson, and F. Hekland. 2008. A Comparison of WirelessHART and ZigBee for Industrial Applications. In *IEEE*. 85.

[Links(2022)] C. Links. 2022. The Evolution of Wi-Fi networks: from IEEE 802.11 to Wi-Fi 6E. Available: https://cloudsecurityalliance.org/2023.

[Lueth(2023)] Knud Lasse Lueth. 2023. Winning in IoT: How the enterprise IoT market is evolving. (2023). https://iot-analytics.com/how-enterprise-iot-market-is-evolving/ Accessed: 2023-06-07.

[Mahnke et al.(2009)] W. Mahnke, S.-H. Leitner, and M. Damm. 2009. *OPC Unified Architecture*. Springer Science & Business Media.

[Market Research Future(2024)] Market Research Future. 2024. Global Wireless Connectivity Market Overview. https://www.marketresearchfuture.com/reports/wireless-connectivity-market-2148

[Masse(2011)] M. Masse. 2011. *REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces*. O'Reilly Media, Inc.

[MITRE Corporation(2023)] MITRE Corporation. 2023. *CVE - Common Vulnerabilities and Exposures*. https://cve.mitre.org/

[Mubashar et al.(2021)] R. Mubashar, MAB. Siddique, AU. Rehman, A. Asad, and Asad Rasool. 2021. Comparative performance analysis of short-range wireless protocols for wireless personal area network. *Iran Journal of Computer Science* 4 (2021), 201–210.

[Naik(2017)] N. Naik. 2017. Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP. In *IEEE*. 1–7.

[Nalin(2021)] Michela Nalin. 2021. *Continued growth for industrial networks despite pandemic - Industrial network market shares 2021 according to HMS Networks*. https://www.pandct.com/news/continued-growth-for-industrial-networks-despite-pandemic-industrial-network-market-shares-2021-according-to-hms-networks/13/04/2021

[National Institute of Standards and Technology(2023)] National Institute of Standards and Technology. 2023. *National Vulnerability Database*. https://nvd.nist.gov/vuln/

[Network(2023)] The Things Network. 2023. What are LoRa and LoRaWAN? Available: https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/2023.

[Neumann and Poschmann(2005)] P. Neumann and A. Poschmann. 2005. Ethernet-Based Real-Time Communications with PROFINET IO. *WSEAS Transactions on Communications* 4, 5 (2005), 235–245.

[Newark(2023)] Newark. 2023. IoT Wireless Network Protocols. Available: https://www.newark.com/iot-wireless-network-protocols.

[Nguyen et al.(2015)] KT. Nguyen, L. Maryline, and O. Nouha. 2015. Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks* 32 (2015), 17–31.

[OASIS(2023)] OASIS. 2023. MQTT- The Standard for IoT Messaging. Available: https://mqtt.org/2023.

[Olson(2019)] E. Olson. 2019. *What is the most popular industrial network protocol?* https://insights.globalspec.com/article/11936/what-is-the-most-popular-industrial-network-protocol

[Oza(2019)] T. Oza. 2019. A Comparison of Common Industrial IoT Protocols. (2019). https://www.mpdigest.com/2019/11/22/a-comparison-of-common-industrial-iot-protocols/

[Pahlavan and Krishnamurthy(2009)] K. Pahlavan and P. Krishnamurthy. 2009. *Networking Fundamentals: Wide, Local and Personal Area Communications*. John Wiley & Sons.

[Pahlavan and Krishnamurthy(2013)] K. Pahlavan and P. Krishnamurthy. 2013. *Principles of Wireless Access and Localization*. John Wiley & Sons.
[Peterson and Davie(2007)] L.L. Peterson and B.S. Davie. 2007. *Computer Networks: A Systems Approach*. Elsevier.
[Pimentel and Schneider(2016)] J. Pimentel and G. Schneider. 2016. Network Topology Protocol Change from ControlNetTM to Ethernet/IPTM for a Master Control Station in a Subsea Production System.
[Rostan et al.(2024)] Martin Rostan et al. 2024. Industrial Ethernet Technologies. Available: https://www.ethercat.org/download/documents/Industrial_Ethernet_Technologies.pdf.
[Shuka(2023)] S. Shuka. 2023. Wi-Fi: Basics, History, Types, and Internet Connections. Available: https://www.myprostatus.com/wi-fi-basics-history-types-and-internet-connections/.
[SIEMENS(2023)] SIEMENS. 2023. What Properties, Advantages and Special Features Does the S7 Protocol Offer? Available: https://support.industry.siemens.com/cs/document/26483647/what-properties-advantages-and-special-features-does-the-s7-protocol-offer-?dti=0\&lc=en-WW.
[Staff(2023)] Editorial Staff. 2023. DNP3 Communication Protocol Overview. Available: https://instrumentationtools.com/dnp3-communication-protocol-overview/2023.
[Tanenbaum and Wetherall(2010)] A.S. Tanenbaum and D.J. Wetherall. 2010. *Computer Networks*. Prentice Hall Press.
[unabiz(2024)] unabiz. 2024. What is Sigfox? Available: https://www.sigfox.com/what-is-sigfox/.
[Vora(2015)] L. J. Vora. 2015. Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G. *International Journal of Modern Trends in Engineering and Research* 2, 10 (2015), 281–290.
[Wood(2024)] Laura Wood. 2024. Global Wireless Connectivity Market Assessment 2024-2031. https://www.globenewswire.com/news-release/2024/07/30/2920878/28124/en/Global-Wireless-Connectivity-Market-Assessment-2024-2031-Rapid-Expansion-of-Smart-Cities-Globally-and-Rising-Adoption-of-Connected-Vehicles-Driving-the-Market-Totalling-236-6-Billi.html
[world(2022)] IIoT world. 2022. MQTT Widely Used in IIoT. *IIoT world* (2022). https://www.iiot-world.com/industrial-iot/connected-industry/survey-results-mqtt-widely-used-in-iiot/

APPENDIX

In this Appendix identified CWE's are described [National Institute of Standards and Technology(2023)]:

- CWE-20: Improper Input Validation
- CWE-77: Command Injection
- CWE-78: OS Command Injection
- CWE-79: Cross-site Scripting
- CWE-119: Improper Restriction of Operations within the bounds of a memory buffer
- CWE-120: Classic Buffer Overflow
- CWE-125: Out-of-Bounds Read
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
- CWE-287: Improper Authentication
- CWE-295: Improper Certificate Validation
- CWE-306: Missing Authentication for Critical Function
- CWE-310: Cryptographic Issues
- CWE-399: Resource Management Errors
- CWE-400: Resource Exhaustion
- CWE-476: Null Pointer Dereference
- CWE-611: Improper Restriction of XML External Entity Reference ('XXE')
- CWE-754: Improper Check for Exceptional Conditions
- CWE-787: Out-of-Bounds Write
- CWE-862: Missing Authorization

Dr. Maryam Karimi (IEEE Senior Member), is a Post-Doctoral Research Scientist in the innovation and future of industry research group at FM, where she created a testbed and is conducting research in security and vulnerabilities of industrial IoT. She received her Ph.D. at the University of Pittsburgh in the Department of Informatics and Networked Systems in the School of Computing and Information. She is also a holder of the CISSP and CC certificates, demonstrating her expertise in the field of information security. Her thesis was on security of the internet of things (IoT) and Software Defined Network (SDN) for which she achieved second place in the ACM graduate research competition at the Grace Hopper conference 2019. Her expertise in computer science has led to numerous publications in top conferences such as CCGRID, ACM MSWIM, IEEE LCN, and others. She is also the winner of the first place in the international RoboCup competition in 2014. Her research interests span a wide range of topics, including security, Internet of Things, wireless networks, Software Defined Networks, and applied machine learning.

Dr. Roland Shaefer is Research Area Director and a leading researcher in FM, focusing on automation and digitalization in business worldwide. He oversees global research on system-level risks, including those related to automated warehousing and logistics, information networking, and cybersecurity systems. Additionally, His work delves into subsystem and component-related risks associated with energy storage, control and monitoring systems, and charging systems, among others. Prior to joining FM, he was VP of Innovation Management at Balluff GmbH, a developer of automation technology products, where he also held positions including Director of Operations and Manager of Corporate Industrial Engineering. Roland brings expertise in electronics, mechanics, optics, software and IT, as well as international experience in research, innovation and production technology, to this position. He also holds 10 patents. Roland has a Bachelor of Science in electrical engineering from the University of Alberta and master's and doctorate degrees in electrical and computer engineering from Carnegie Mellon University, as well as an MBA from the Open University.