The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2021

Volume 14, Pages 57-65

IConTech 2021: International Conference on Technology

A Comparative Study on Industrial Communication Protocols Using IoT Platforms

Arda KOCAMUFTUOGLU
R&D Center
Klemsan Electric Electronics

Okan AKBAY
R&D Center
Klemsan Electric Electronics

Serkan KABA
R&D Center
Klemsan Electric Electronics

Abstract: In this study, the industrial communication protocols used in internet of things platforms are explained and compared with respect to pre-defined metrics which are gathered from devices in the industrial area, communication protocol principles, customer feedback and device hardware capabilities. They are explained in detail for end users and systems. Communication protocols in industrial area are given and illustrated with comparative table. The presented information and comparisons provide guidance for industrial internet of things projects. The selection of communication protocol is a critical process for surviving and sustaining of IoT platforms. IoT platforms provide solutions for industrial area for both on premise and cloud based applications compatible with industrial communication protocols. This study is shaped by the IoT platform which is developed by Klemsan, improved by industrial communication protocols which are widely used in industrial area, are explained briefly. There are 13 evaluation metrics which are presented in detail that is necessary to be chosen between industrial communication protocols for IoT platforms.

Keywords: Communication, Protocol, Internet of things

Introduction

Digital communication is comprised of distributed computer control systems in both production lines and process control. Launching of wired systems and deployment of distributed industrial automation systems give importance to device autonomy and decentralized decision-making and control loops.

Today, wired systems are standardized and they are the most important communication systems used in commercial control installations. On the other hand, Ethernet is one of the most important communication technologies in the office space. For this reason, the usage of Ethernet is widespread in the industrial applications. Besides, Ethernet based (wired) industrial communication protocols are utilized in the industrial automations, the use of wireless technologies in the industrial area is also increasing, and thus heterogeneous networks are getting better included wired and wireless communication systems as well as local and wide area networks.

Various communication protocols have evolved due to the development of network structures and communication technologies and thus these protocols bring connected devices to access Internet gathering their measurement values into IoT (Internet of Things) platforms. This causes some problems such as speed, complexity, bandwidth, connection distances and data quality. This paper illustrates the commonly used industrial communication protocols in IoT platforms.

Communication Protocols

Data communication is the transfer of an information or data between a transmitter and a receiver as digital or analogous via connection element. Communication protocols are used in the industry to connect various control devices (Online, 2019). Industrial automation control systems such as SCADA (Supervisory Control and Data Acquisition), PLC (Programmable Logic Controller) and DCS (Distributed Control System) use various communication protocols to transfer data collecting from the shop floor to the related software tools and external systems.

Industrial communication protocols provide data communication over a certain communication standard and network. The most commonly used interaction models of communication protocols are request/response and publish/subscribe (Dizdarevic, Carpio, Jukan, & Bruin, 2019). Each communication protocol specializes in a private task and their usage depends on the application. A protocol cannot meet all the requirements of a complex application and eventually multiple protocols are combined. For this reason, complex applications transform into OPC UA (Open Platform Communication and Unified Architecture) and DDS (Data Distribution Service) with the development of Industry 4.0 applications.

Internet of Things

Internet of Things refers to the interconnection of uniquely identifiable devices within the existing internet infrastructure. Internet of Things are smart services and applications that facilitates people's living standards (Gündüz & Daş, 2018). Moreover, Internet of Things can be called smart network device systems that connect and share information with various communication protocols (Altınpulluk, 2018). Internet of Things concept which includes objects managed via the Internet, known as M2M (Machine-to-Machine) technology in the history. Furthermore, Internet of Things concept is expected to go beyond M2M communication to offer advanced connectivity to devices, systems and services through a variety of protocols.

Sensors, embedded devices and the Internet used in internet of things will disrupt the transformation in production area. Moreover, robotics and artificial intelligence techniques used in shop floor area provide added-value to the companies in terms of quality and speed, on the other hand, RFID technologies used in logistics and raw materials will be a beneficial method for products to reach the end users and customers in the supply chain (Öz & Arslan, 2019). Furthermore, Internet of things is the methodology that enables the application processes to be controlled at the high level by connecting smart device to the Internet.

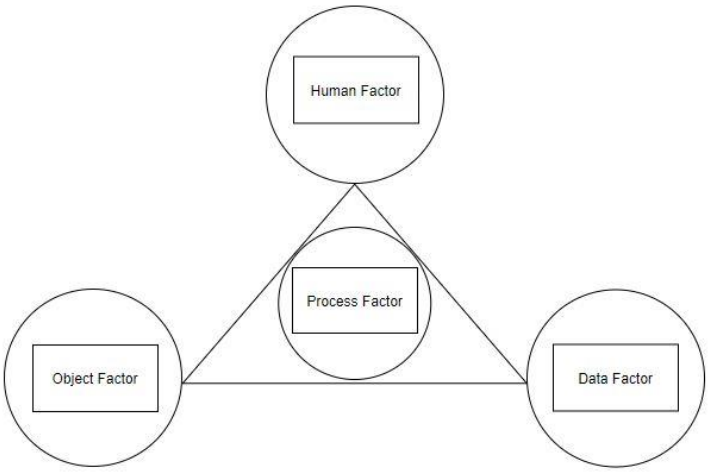

Figure 1. IOT Factors

Internet of things consists of four main factors. Fig. 1 shows these four factors. The human factor is necessary to make the data meaningful and analyze it from objects (devices). Object factor is a device or sensor which is connected to the Internet, generates data in the shop floor. The data factor is the structured or unstructured clusters produced by the objects (devices) in the production. This data becomes a big data by hosting in local, central or distributed servers. The process factor is a process that provides interaction and interoperability between object, human and data.Internet of things can be applied to many sectors. IoT appears in smart home and building automation, smart wearable technologies, smart energy, smart cities, smart agriculture and health applications.

IoT Platform

IoT platform provides the necessary infrastructure for all the services such as data storage, inter-connected device communication, device configuration and various software services. There are three basic service principles in IoT platforms; software as a service (SAAS), platform as a service (PAAS) and infrastructure as a service (IAAS). IoT platforms are deployed both on premise and cloud based.

IoT platforms have some advantages from SCADA systems in production and industrial facilities (IOT Online, 2021).

- Interoperability of the devices
- Data analysis and interpretation
- Scalability
- Standards and protocols
- Cost

As Klemsan, KIO (Klemsan Internet Objects) which we have developed in-house, offers solutions to the customers in the field of energy efficiency and savings. KIO IoT platform can communicate with energy measurement devices, sensors, input / output units, electricity, water, natural gas and heat meters by adding brand-independent structure.

KIO is located at a position in Fig. 2 in vertical integration. Not only collecting data of the devices in shop floor, but also transferring data to KIO via PLC or SCADA. KIO IoT platform which can also be integrated with MES (Manufacturing Execution System) and ERP (Enterprise Resource Planning) systems, can provide data transfer to these systems via web services.

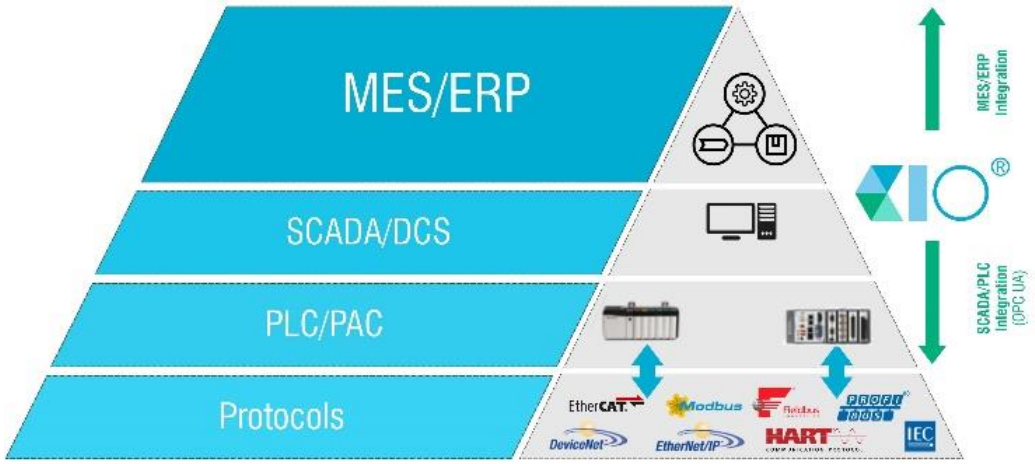

Figure 2. Vertical integration in KIO

Industrial Communication Protocols in IoT Platform

As Klemsan, KIO supports industrial communication protocols collecting data from production area. The protocols that are used in KIO IoT platform listed below.

Modbus

Modbus is a serial communication protocol developed by Modicon in 1979 for use with PLCs (Modbus Online, 2020). Modbus protocol provides solutions for serial and Ethernet based communication. Modbus RTU (Remote Telemetry Unit) is used for serial communication, Modbus TCP/IP (Transmission Control Protocol/Internet Protocol) is used for Ethernet communication. Modbus TCP/IP uses TCP/IP model to move data of the Modbus message structure between compatible devices. Modbus TCP/IP message is a simple Modbus communication encapsulated in a TCP/IP packet (Irmak & Erkek, 2018).

Modbus protocol is the most widely used communication protocol among the industrial communication protocols. There are multiple reasons listed below:

- Simple to understand and integrate with systems / devices
- Master/Slave structure. For example, there is one RS485 (Balance Data Transmission) line including one master and more than one slave devices. The master refers to device / system that needs the data. The slave refers to system that contains the data to be accessed. Due to not requiring any session initiation for communication, querying data can be done at high speed depending on the speed of the communication line.

Another reason for its frequent usage is that there were little alternatives in that period. Today, the usage rate of Modbus TCP/IP is 50% (Modbus IDA Online, 2006).

IEC 60870-5

This protocol was developed by TC (Technical Committee) 57 working group of IEC (International Electro technical Commission) technical committees. TC 57 is responsible for development of the standards for information exchange between power systems and other related systems including energy management systems, SCADA, distribution automation and protection.

IEC 60870-5-101 is the version of protocol that works on serial communication. The version used on TCP/IP is IEC 60870-5-104. Today, the devices whose protocol known as IEC 104 is widely used on RTU (Remote Terminal Unit) devices and electrical grid products. These devices are controlled through SCADA systems.

MQTT

MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol that provides a simple way to distribute telemetry information for resource constrained network clients. The protocol uses publish / subscribe communication model which is determined by M2M communication and plays an important role in IoT (MQTT Online, 2020).

MQTT protocol consists of client and broker. Messages sent by the client are inspected and transmitted with broker. Each message sent by the client is tagged into a topic. The broker separates and sends messages to clients subscribed to the specified topic. The client who wants to forward its message to the relevant recipient, wants to send the recorded message topic to the broker. While a client can subscribe to a topic, more clients can also subscribe to it.

It is the most widely used protocol of today's IoT platform. It is used in IoT platforms with TLS (Transport Layer Security)/SSL (Secure Sockets Layer) security support.

OPC UA

OPC UA is an open standard that determines the exchange of information in industrial communications. This standard applies devices within the machines, between machines and communication with machines and systems that bring together IT (Information Technology) and OT (Operational Technology). OPC was first appeared for working specific standard in Microsoft operating systems. Due to service-oriented architecture and security issues, OPC UA developed with respect to scalable and extensible structure including open platform architecture (OPC Online, 2020).

OPC UA is a suitable standard for closed network or over the Internet. Security is guaranteed by embedded protocol in the form of authentication and encryption in access control (OPC Online, 2018).

Comparison Metrics for Industrial Communication Protocols in IoT Platform

As Klemsan, our IoT platform supports industrial communication protocols explained above. These protocols are widespread and valid protocols in industrial automation area. We state that we make out some metrics for comparison in industrial communication protocols experienced in our IoT platform.

Finding Versions That Can Run on Serial Communication and TCP/IP

When a device or a sensor has been developed for the first time, the device or the sensor which has similar functions, should be searched in the market. If the device is specified for development, communication protocol should also be evaluated with widely usage and compatibility. Communication protocol is an important factor to specify hardware costs. If the device is designed as cost-oriented, it should be chosen as serial communication, otherwise it runs on TCP/IP side with the communication interface such as Ethernet, Wifi or GSM. Nowadays, manufacturers start to add both serial communication and TCP/IP versions for communication protocols. Communication protocols for both serial communication and TCP/IP versions are shown in the below table.

Table 1. Communication protocols for serial and tcp/ip

Serial Communication	TCP/IP Communication
Modbus RTU / Modbus ASCII	Modbus TCP
IEC60870-5-101	IEC60870-5-104
Profibus	ProfiNET
EtherCAT	EtherNET/IP

No Need for Static IP

Serial communication can be considered as a permanent cable between two devices. This cable length can be 30 cm or kilometers. Since the communication line is always available in serial communication, data exchange can be done at any time. On the other hand, a virtual cable/bridge should be established in TCP/IP world so that the systems communicate with each other. The bridge is known as a socket connection. The socket connection uses many applications such as web sites, mobile application and database connection. A server and a client software are required in order to establish the socket connection. Connection direction is from clients to server. For this reason, clients must know the server's IP address to connect to the server. Today, there are thousands of servers on the Internet. Not only knowing of the IP adress is enough, but also communication port is used for communication. There is not any restriction as only one communication protocol will work on the servers. A total of 65536 ports can be opened on a server.

In some conditions, static IP is needed when connecting to high number of devices in some communication protocols. For example, if the devices connect with the communication protocols as Modbus TCP/IP in the local network or on the Internet, the device must have an unchangeable static IP. In this case, port forwarding will be able to be done on the modem/router.

Internet static IP is not preferred in GSM (Global System for Mobile Communications)-based systems due to both cost and security reasons. Enterprise private APNs (Access Point Name) are the most widely used M2M communication type. The biggest problem of private APNs is the difficulty in operation management. If the system includes 10000 SIM (Subscriber Identity Module) cards, this is very hard to manage for businesses. The most comfortable and simple management systems with high point numbers to choose devices and protocols that do not need static IP.

Some communication protocols do not require static IP. MQTT is an example protocol that uses dynamic IP. MQTT clients (device, sensor, central software) are only connected to Broker service over the socket connection. All MQTT clients can be found in dynamic IP in the system where this protocol is used.

One of the biggest problems of the protocols that need static IP is security. All applications in the network can request a socket connection to the server which includes devices without an IP restriction. In this case, unwanted situations may occur with attacks. In industrial facilities, static IP does not cause a great risk as it is solved in the local network and is not opened on the Internet. However, a penetration into network may affect the devices which have static IPs of the local network.

Session Based Communication

Security is one of the most important criteria in the selection of the communication protocol. Attacks from unknown resources can cause the system to be in undesirable situations. The system can be made more secure with session management in some protocols. Unwanted access can be prevented by a session to any device or broker. Session should be started with a username and a password. Some systems only require a password. Although session management is beneficial for security, a username and a password can be stolen with network sniffing tools.

TLS/SSL Based High-Level Security

Security is an inevitable feature for a communication protocol. TLS is the current and updated version of SSL. TLS/SSL option maximizes the security of the protocol. Today, TLS/SSL option is available in many protocols such as IEC 60870-5, OPC UA and MQTT. On the other hand, Modbus protocol has existed without TLS/SSL for many years. Few manufacturers have added TLS/SSL option to their systems.

Disconnection Detection Mechanism

While the protocols are working in the communication layers, communication problems may occur due to the fact that connection breaks are not detected in some cases. The most common example of this situation occurs in GSM communication. These breaks can be detected late in the devices on which the protocol works. In order to prevent this situation, manufacturers take extra precautions. In protocols such as MQTT, two extra connections are kept for communication health status control. In one of these two connections, the client tests its connection to the broker. In the other connection, the broker checks its connection to the client. If there is no data exchange during the periods of non-communication intervals, both parties understand that the connection between each other has been broken.

Data Size Optimization

High data traffic is observed in communication systems. The data download and upload amount of a device in Modbus TCP/IP protocol is as much as the communication with the application requesting data from this device. Multiple interrogations of this device can double the amount of the data. If the device was developed with a cost-oriented approach, there may even be a single socket operation of the device. The best method is to minimize the communication with the device in such cases. As in MQTT protocol, If all clients are only in communication with the broker, the communication with the devices in the field will be reduced to minimum levels.

Quality of Service Support

It is a metric seen in advanced level communication protocols. A quality information is assigned to each message with the data in protocols such as IEC 60870-5 and MQTT. It is possible for each message to be successfully delivered to the clients one, as well as for non-critical messages to be delivered or not delivered one or more times in order to not to occupy the network traffic.

Lightweight

It is very important that the protocol is simple and can run on the lowest hardware resources in the industry. This is one of the most important details in the usage of Modbus protocol. Despite its advanced structure in

MQTT protocol, it can work with low hardware resources. However, since some protocols were developed without considering this basic requirement, it is not possible to become widespread.

Availability of Open Source Libraries in Programming Languages for Communication Protocols

Protocols and their standards are created by organizations and commissions such as IEC. After the development process of the protocols, commissions such as IEC sell the technical details of the protocols on the web site for a fee. After these technical documents are purchased and examined, the implementation of the protocol on a device takes a long time. Therefore, this technical document is very hard to understand and difficult to implement for producing new devices. For this reason, some protocols are simple to embed for the devices and can be accessed over the Internet. There are many simulation programs such as Modbus protocol. On the other hand, MQTT protocol has become widespread as well as its many advanced features. The technical documents of MQTT protocol can be obtained from the Internet supported by giant technology companies such as IBM (International Business Machines). Moreover, open source libraries for each programming language can be downloaded freely and turned into distributable software packages.

Communication Pattern

There are two types of communication patterns in insdutrial communication protocols which are request / response and publish / subscribe. Modbus and OPC UA protocols only use request / response structure. Not only IEC60870-5 protocol has “request / response” structure, but also it has “ send when value changes”. On the contrary, MQTT protocol has publish / subscribe structure. MQTT client automatically sends the data to the broker at certain periods or when the value changes.

Bidirectional Communication

Regarding to communication protocols, bidirectional communication can be considered in two different ways:

- Reading data from the field and writing the data to the field (sending command)
- While sending data from the field to the center / server, it is possible to send data from the center / server to the field at the same time.

Both ways provide bidirectional communication. However, the first way is a common structure in all communication protocols. The second way is known as an asynchronous communication. For instance, while a 2 MB file is transmitted from the client to the broker, a subscribed message can be transferred from the broker to the client at the same time.

Timestamp Based Data Transmission and Data Pools

Timestamp data transmission has been developed to eliminate the problem of not being able to transfer data at a certain time interval due to the lack of communication. In this case, data is accumalted in a data pool and transmitted to the center after the communication returns to normal. This feature is not included in every protocol. IEC 60870-5 has this feature. Owing to this structure, data loss are prevented for certain levels as a result of communication breaks.

Continuous Improvement

This is a necessary metric for today’s industrial communication protocols. The protocol which is alive, is continued to be developed showing that it is still being invested and new features are being added. Many protocols lose their updates as they complete the development phase. On the other hand, MQTT protocol continues to be developed with version five in the current situation.

All metrics are shown in one table in the following. It is overviewed and seen briefly. The rows in the table represent the metrics of industrial communication protocols. The columns in the table represent the

communication protocols that are stated in this study. It is analyzed that IEC 60870-5 and MQTT protocols are supporting metrics for almost all.

Table 2. Comparison table for communication protocols

Metrics	MOBUS	IEC 60870-5	OPC UA	MQTT
Finding versions that can run on serial communications and TCP-UP	✓	✓		
No need for static IP				✓
Session based communications		✓	✓	✓
TLS-SSL based high-level security		✓	✓	✓
Disconnection detection mechanism		✓	✓	✓
Data size optimization				✓
Quality of service support		✓		✓
Lightweight	✓			✓
Availability of open source libraries in programming languages for communication protocols	✓			✓
Communication pattern	✓	✓	✓	✓
Bidirectional communication		✓		✓
Timestamp based data transmission and data pools		✓		
Continuous improvement				✓

Results

Communication protocol selection is a critical process. Selection of communication protocols; it is a decision that needs to be performed when a new device is developed, when an existing device needs to be improved or when scoping an IOT system at the initial stage. As Klemsan, our IOT platform (KIO) which supported Modbus and IEC62056-21, was first introduced to the market. Afterwards, OPC UA and MQTT protocols were added to the platform according to market research and customer requests. Nowadays, our platform communicates many industrial devices with supporting the variety of industrial communication protocols. Devices with many communication protocols in the field start to connect to the outside world over OPC UA with supported devices or MQTT with hardware gateways. For this reason, it is expected that MQTT will become widespread in the market.

In this study, the widely used industrial communication protocols in IOT platforms have been explained and compared with respect to some metrics. There are important metrics that shows us to choose industrial communication protocols which are compatible with IOT platforms. Security, structure of data, communication infrastructure, and continuous improvement are the critical factors to be chosen communication protocol in industrial area. SCADA is still preferred application in the industry, for this reason IEC 60870-5 protocol meets communication protocol metrics. In addition, MQTT protocol has almost metrics to be chosen for generating a new device or implementing in IOT platform. Learning the protocol, implementing it on a software or a device is one of the most accurate decisions for the companies.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors

References

Akademi 4.0 Ekibi (17 February 2020). *OPC Nedir?*. https://www.akademi40.org/opc-nedir

Altınpulluk, H. (2018). Nesnelerin interneti teknolojisinin eğitim ortamlarında kullanımı. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, *4*(1), 94-111.

Dizdarević, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2019). A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. *ACM Computing Surveys (CSUR)*, *51*(6), 1-29.

Gündüz, M. Z., & Das, R. (2018). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, *24*(2), 327-335.

GSL (24 September 2018). *Dijital Çevrim Çağında OPC UA: Nedir, Neden Kullanılır?*. https://www.gsl.com.tr/blog/dijital-devrim-caginda-opc-ua-nedir-neden-kullanlr.

Hubbox (2020). *MODBUS Protokolü ve tüm özellikleri nelerdir?*. https://www.hubbox.io/tr/blog/veri-toplama/modbus-protokolu-ve-tum-ozellikleri-nedir.

Irmak, E., & Erkek, İ. (2018). Endüstriyel Kontrol Sistemleri ve SCADA Uygulamalarının Siber Güvenliği: Modbus TCP Protokolü Örneği. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, *6*(1), 1-16.

Modbus (28 December 2006). *Modbus IDA, Modbus Application Protocol* https://modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

Nesnelerin İnterneti ve Endüstriyel Uygulamaları. (2020) (online) Available: https://www.siskon.com.tr/dosya/PDF/Makale/Nesnelerin_Interneti_ve_Endustriyel_Uygulamalar.docx

Öz, A, & Arslan, B. (2019). Marketing 5.0: Internet of Things Marketing. *Journal of Strategic Research in Social Science*, *5*(1), 243-266.

Roltek (29 March 2021) *IOT Platform ve SCADA: Karşılaştırmalı Analiz*. https://www.roltek.com.tr/blog/iot-platform-vs-scada-karsilastirmali-analiz/.

Siscon (2020). *Neden bir Nesnelerin İnterneti (IoT) Platformu kullanmalısınız?* (2020). https://www.innova.com.tr/tr/blog/dijital-donusum-blog/neden-bir-nesnelerin-interneti-iot-platformu-kullanmalisiniz

Stendustri Otomasyon Dergisi (16 May 2019). *Endüstriyel Haberleşme Protokolleri,* https://www.stendustri.com.tr/otomasyon/endustriyel-haberlesme-protokolleri-h100528.html.

Volsoft (2020) *MQTT Nedir?*. https://www.thingson.io/mqtt-nedir/.

Author Information

Arda KOCAMUFTUOGLU
R&D Center Klemsan Electric Electronics
Izmir, Turkey
Contact e-mail: ardakocamuftuoglu@klemsan.com.tr

Okan AKBAY
R&D Center Klemsan Electric Electronics
Izmir, Turkey

Serkan KABA
R&D Center Klemsan Electric Electronics
Izmir, Turkey

To cite this article:

Kocamuftuoglu, A., Akbay, O., & Kaba, S. (2021). A comparative study on industrial communication protocols using IoT platforms. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 14*, 57-65.