5th Conference on Production Systems and Logistics

A systematic literature review of communications standards in discrete manufacturing

Furkan Ercan[1], Maximilian Bega[1], Bernd Kuhlenkötter[1]

[1]*Chair of Production Systems / Ruhr-University Bochum, Bochum, Germany*

Abstract

Industry 4.0 has a particular emphasis on the data landscape of production facilities. Data is needed to gain essential insights from the production machinery to support operations management in better decision-making or indirectly by feeding decision support systems. Such data is encapsulated in an industrial communication standard to organize in a higher-level ontology. It is challenging for operation technology specialists to have an overview of all those standards because they are numerous. This work contributes a solution to this problem by systematically approaching the literature to give an overview of the industrial communication standards landscape. The method used is a systematic literature review with a backward and forward search consisting of three main phases: 1. keyword-based search on different platforms, 2. abstract screening, and 3. full-text screening. Over 2,100 article abstracts have been parsed systematically to condense it to the most relevant 309 full-text articles. This work presents an overview of the most significant industrial communication standards mentioned in these articles. Several use cases and some brief IT-security-relevant aspects are presented as well.

Keywords: Industry 4.0; communication standards; systematic literature review; ProfiNet; Modbus; MQTT; OPC UA; MTConnect

1. Introduction

Industrial communication standards have seen significant advancements in recent years, with the emergence of Industry 4.0 and the (Industrial) Internet of Things (IIoT). As a result, many communication standards are available for use in industrial manufacturing settings, each with its strengths and weaknesses. This paper aims to compare the most common industrial communication standards comprehensively. By examining each standard's practical applicability and popularity, valuable insights to researchers and practitioners in data-driven manufacturing are offered. The technical details and the distribution of the chosen standard are essential criteria for selection from the plethora of industrial communication standards.

The Open System Interconnection (OSI) reference model provides an essential structure for classifying communication systems. It defines seven different layers. Starting with the physical layer, where electromechanical properties of the interface are described, and ending with the application layer, where the interface to the software application is defined. All standards mentioned in this paper operate at the highest level of abstraction, the application layer. The underlying layers are outside the scope of the industrial communication standards.

2. Related Work

Several other authors have reviewed industrial communication standards. Hasnain and Awais [1] classified wireless IoT protocols and proposed a three-dimensional network design space with battery life, gateway

DOI: https://doi.org/10.15488/15260
ISSN: 2701-6277

range, and the device data rate as parameters as a decision aid. They focus their work on wireless protocols. Lata and Kumar [2] classified protocols for an IoT environment based on a five-layer structure from the Internet Protocol for Smart Objects Alliance (IPSO). Additionally, they have provided several examples of IoT-based applications. They conclude their work by stating that several intervening protocols are required to form a holistic IoT architecture. Gericke et al. [3] reviewed communication protocols within a cloud manufacturing environment and sorted protocols into different layers. They analyzed a cloud-based manufacturing system consisting of three communication layers: The first is between a cloud and a server, the second between server and manufacturing units, and the third between the manufacturing units. They provide examples of communication protocols for each of the three layers.

Pliatsios et al. [4] examine protocols in their survey with an extensive focus on security. They give an overview of Supervisory Control and Data Acquisition (SCADA) systems' general architecture, describe communication protocols, discuss security incidents, and review security proposals for critical infrastructure.

The main shortcoming of the above mentioned works is that they do not describe a systematic approach to filter the relevant protocols from the literature corpus. This shortcoming motivated this review.

3. Methodology

For pointing out relevant literature regarding industrial communication standards, the systematic literature research (SLR) approach introduced by Brunton and Thomas [5] was used. Figure 1 shows the search query and illustrates the quantitative results of the literature search (only scientific publications, other sources (e.g. norms) are omitted).

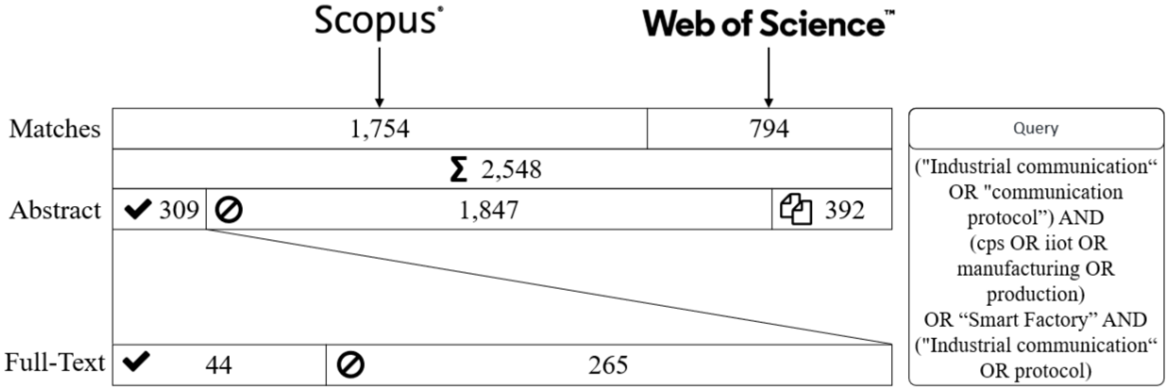
Scopus
Web of Science
Matches
1,754
794
Σ 2,548
Abstract
✓ 309
1,847
392
Full-Text
✓ 44
265
Query
("Industrial communication" OR "communication protocol") AND (cps OR iiot OR manufacturing OR production) OR "Smart Factory" AND ("Industrial communication" OR protocol)

Figure 1: Results of the literature search and the search query

First, broad search queries were defined to gather all publications that treat the application of communication standards within the production environment.

Two scientific databases, Scopus and Web of Science, were searched without any limitations on publication date. All publications up to March 2023 were taken into consideration. Furthermore, only publications in English and German were included. Overall, 2,156 publications were gathered, and double abstract screening for each publication was performed, meaning a publication is only suitable for subsequent full-text review when both reviewers agreed. After directly eliminating 1,847 publications and solving 467 reviewer derivations, 309 publications were included in the full-text review. Finally, the publications were categorized into five standards: MTConnect, MQTT, OPC UA, Modbus, and ProfiNet.

4. Results

In this Chapter, the results of the literature search are shown. Each protocol is introduced, and related use cases are presented.

4.1 MTConnect

MTConnect is a royalty-free, read-only, open-source standard that unifies over 250,000 devices across multiple industries [6]. Its goal is to provide structured, contextual data without a proprietary format by defining a semantic data model and an extensible data dictionary. The standard employs the Hypertext Transfer Protocol (HTTP) as a means of transportation and Extensible Markup Language (XML) as the encoding mechanism. There are three basic building blocks defined in the standard: The device that generates the Data, an agent that provides a representational state transfer (REST) interface, and a client software application [5]. MTConnect is typically used for machine monitoring since it is a read-only protocol.

Numerous use cases of MTConnect are discussed in scientific literature. Lee et al. [7] developed a monitoring system to track the axis positions of a virtual milling machine. This system is similar to the event-based real-time control architecture for tool-tip temperature control of a small-scale CNC prototype machine demonstrated in the work of Subhasish Malik et al. [8], Edrington et al. [9] built a web-based application for general-purpose machine monitoring.

4.2 MQTT

In contrast to MTConnect, MQTT is bi-directional, lightweight, stateful, and standardized by ISO 20922 [10]. By default, it uses the Transmission Control Protocol (TCP) for transmission but can be configured to use non-TCP protocols such as Zigbee, User Datagram Protocol (UDP), or Bluetooth. The architecture of MQTT is based on a client-server and publish-subscribe paradigm (see Figure 2). The MQTT broker is the central access point between clients. The broker is a central node that forwards all messages; clients cannot communicate directly. Several open-source MQTT broker implementations on different platforms exist (for a comparison, see [10]). The communication architecture is shown in Figure 2 Clients subscribe to a specific topic structure, similar to a path in a file system, e.g. "productionfacility/shopfloor/millingmachine/cuttingvelocity/"; a publisher sends the values to the topic, and a subscriber receives the values. A unique feature is that MQTT guarantees a particular quality of service (QoS), which can be chosen between three levels: At level 0, the publisher sends the message once, and no confirmation from the subscriber is expected. At levels 1 and 2, the subscriber must confirm with a 2-part or a 4-part handshake that the message arrived successfully.

Since MQTT lacks a systematic way to represent data, the Eclipse Foundation developed an extension specification to address this issue: SparkPlug [11]. The Eclipse SparkPlug Working Group unified the topic name scheme, data, message types, session management and introduced command messages.

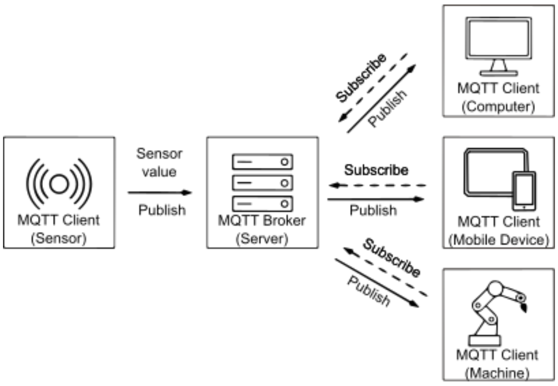

Figure 2: Network architecture of MQTT [7]

The scientific literature highlights various use cases for MQTT. For instance, Salvatierra et al. [12] and Ahmad et al. [13] designed a condition monitoring system for a milling machine. Breuning et al. [14] presented a model-driven approach to aggregate data in production networks with a heterogeneous protocol landscape. Aliev et al. [15] implemented real-time monitoring of critical metrics customized to collaborative and mobile robotics. Bartholet et al. [16] built a multi-protocol bridge that unifies OPC UA and MQTT through a REST Interface. Yeh et al. [17] made a gesture recognition application that employed edge computing to classify gestures and send appropriate requests to a machine via MQTT. Luchian et al. [18] utilized the collaborative IoT framework Coaty to implement field devices and controllers.

4.3 OPC UA

Open Platform Communications Unified Architecture (OPC UA) is an open standard focusing on interoperability, security, extensibility, and reliability [19]. The Reference Architecture Model Industry 4.0 (RAMI 4.0) recommends OPC UA as the only recommended standard in the communication layer [20].

OPC UA provides three different security modes to meet industry standards: “None” for no security, “Sign” for providing authenticity, and “SignAndEncrypt,” which provides authenticity and encrypts the data so that it can only be read by the certificate owner [21].

OPC UA provides two communication mechanisms: client-server and publish-subscribe (PubSub) [22]. In the PubSub model, the clients are not directly connected. In both mechanisms, the network type can either be a brokerless model with UDP broadcasts or a broker-based model. The underlying message protocol can be Advanced Message Queuing Protocol (AMQP) or MQTT.

In a client-server structure, a server implements a set of services and exposes them to a client. The client can then invoke these services. The services are organized into several sets [23]. In addition to services, servers have objects accessible from the address space in various formats. Address spaces structure data systematically so that information models can be used. The data itself can be defined in different encodings (binary, Extensible Markup Language (XML), or JavaScript Object Notation (JSON)). Information models are extending OPC from a communication standard to a shared infrastructure model that facilitates information exchange in a standardized way across all industrial domains and information hierarchies.

The OPC specifications define a basic information model, which is extended by domain-specific information models (e.g. [24]) and standard mappings (e.g. [25]) in the Companion Specifications.

OPC UA consists of an information model that defines the structure and organization of data, a communication model between endpoints, and an extensible conformance model for semantic interoperability.

Numerous OPC use cases are outlined in the literature. For example, Wang et al. [26] proposed a versatile and integrated architecture for the Industrial Internet of Things. Steininger et al. [27] developed a data acquisition system for an experimental deep-drilling setup. Bennulf et al. [28] created a plug-and-produce system that automatically detects and configures the added resources and parts, utilizing OPC UA for communication between system parts. In the mold industry, Martins et al. [29] developed a standardized method for monitoring CNC data, and Kong et al. [30] utilized algorithms to evaluate machine statuses and improve machine utilization. Additionally, Cavalieri and colleagues [31] implemented a platform for accessing OPC UA Servers via the Internet, while Park et al. [32] designed a gateway for legacy equipment.

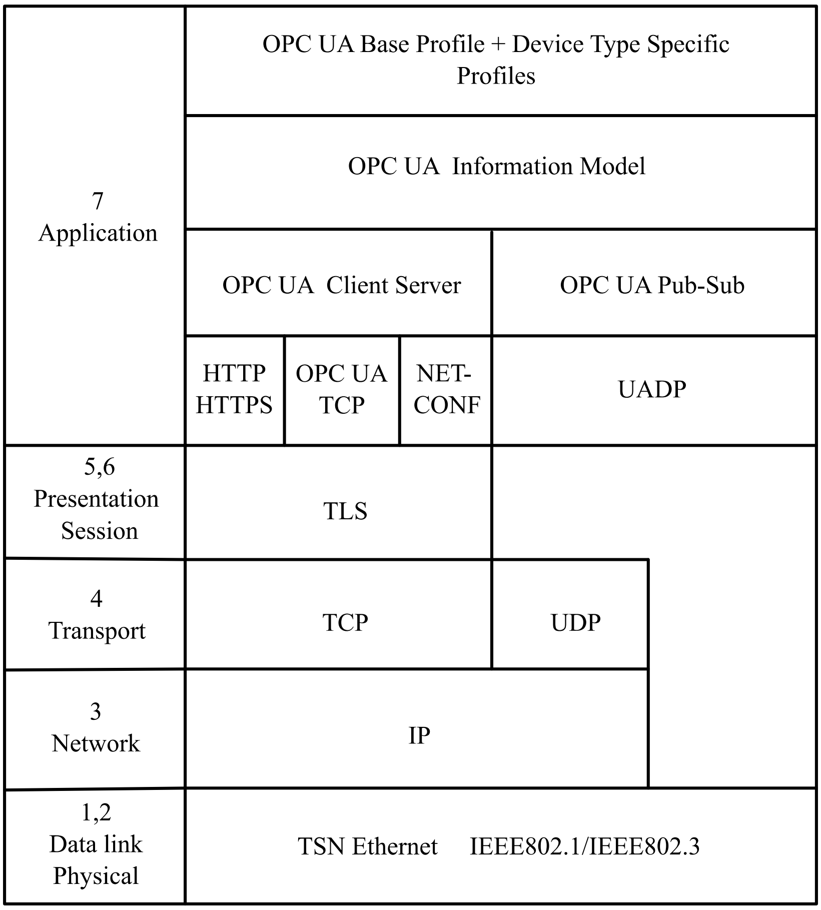

Figure 3: Mapping of OPC UA components to ISO/OSI layers. [33]

4.4 ProfiNet

ProfiNet is an industrial Ethernet standard from the German ProfiBus and ProfiNet International interest group. Devices are classified into three classes: an IO-controller (e.g. Programmable Logic Controller (PLC)), an IO device providing the in-output signals to the process, and an IO-supervisor for configuring the IO-Devices (e.g. a human-machine interface). [34]. A specific file called Generic Station Description (GSD) is provided to ease the configuration process. It is an XML file containing the properties and functions of ProfiNet devices. A GSD file is helpful for virtual facility planning and configuration [35]. An even easier way to configure ProfiNet Devices is described by Duerkop et al. [36], who developed an auto-configurable automation system.

ProfiNet offers several levels of performance. Component-based automation (ProfiNet CBA) provides bus cycle times of 50-100ms with off-the-shelf commercial equipment; for a performance analysis, see [37,38].

In the literature ProfiNet is used in different scenarios. Ionescu et al. designed an autonomous robotic system with a PLC. They use ProfiNet to control and connect the flexible cell to the manufacturing line [39]. A condition monitoring system for rotating machines using ProfiNet is presented by Dias et al. [40].

4.5 Modbus

Even though OPC UA is a modern industrial communication standard, it is not as widely implemented as Modbus [41]. Modbus was developed by Modicon (now Schneider Electric) in 1979 and is independent of the physical interface. Implementations via ZigBee [42], RS485 [43], and virtually in Matlab Simulink [44] are existing. The protocol structure consists of a 1-byte address field, a 1-byte function field, a variable data field, and a 2-byte error check field [45]. The possible function codes for the function field are defined by the Modbus Organization [41].

The most common variants are Modbus Remote Terminal Unit (RTU), Modbus American Standard Code for Information Interchange (ASCII), Modbus Transmission Control Protocol (TCP), and Modbus Plus. Modbus RTU is a binary serial protocol commonly utilized in legacy systems. On the other hand, Modbus ASCII is a serial communication protocol that uses ASCII characters to represent data and is less widely used than Modbus RTU. Meanwhile, Modbus TCP is a request/reply protocol that operates via Ethernet using the Transmission Control Protocol (TCP). It is the most recent variant of Modbus.

Within the scientific literature, Modbus is used for several application scenarios. For instance, Cheng et al. [43] successfully implemented condition monitoring for a wire drawing process using Modbus TCP. Cena et al. [44] developed a Modbus extension for distributed embedded systems by optimizing the protocol's address space size, bandwidth allocation, and handover between masters. Li and Zhong [45] created a gateway between Profibus and Modbus in an aluminum-roasting drought system. Zagan and Găitan [46] measured the performance of Modbus and designed an extension to improve the communication times and dataflow.

5. Discussion

5.1 IT-Security Aspects

Historically grown industrial communication infrastructure is still operated under the assumption that machine and shopfloor communication takes place in isolation from the internet. Due to the advancing networking of the IT- and operation technology infrastructure of a manufacturing company, cybersecurity in industrial networks is decreasing [46,47]. To achieve the full extent of capabilities that are provided by industry 4.0 technologies, the issues surrounding cybersecurity need to be addressed [48] - especially because IIoT devices in their default settings have a higher focus on usability and user experience than on security [49]. Because of its increasing relevance, this article also shortly addresses the topic of cybersecurity. In the following, a selection of different approaches is presented.

Wang et al. [46] described two possible approaches to increase the security of industrial communication standards. First, the addition of cryptographic security mechanisms to the standard itself. Second, the application of an additional encryption protocol such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL). The authors applied this encryption protocol to the Modbus TCP communication standard on a computer platform.

Another Modbus TCP-focused approach used two gateway modules to realize bidirectional data transfer between PLCs and Servers. This concept can be used in legacy systems without a provider dependency [50].

Bienhaus et al. [51] mentioned the use of TLS in combination with MQTT and OPC UA. They integrated TLS and OPC UA in the Trusted Platform Module (TPM) 2.0 framework. Whereas TLS enabled authentication, authorization, cryptography, encryption, and integrity protection, TPM 2.0 was integrated to provide the secure management of cryptographic keys.

However, two contributions focusing on MQTT pointed out that TLS cannot be appropriately used in the Internet of Things due to the limited computing capacity and resources of IoT devices - more lightweight encryption standards are needed [49,52]. Boppana et al. [49] emphasized the danger of man-in-the-middle (MITM) and cross-site scripting (XSS) attacks on IoT devices that use MQTT under default settings. Generally, Kant [53] presented a comprehensive analysis of the cybersecurity of the MQTT communication standard.

Regarding the default security settings in IoT devices, Kohnhäuser et al. [54] addressed this issue in OPC UA – they provided a holistic assessment of existing OPC UA-related secure device provisioning solutions due to the high expected longevity of CPPS. Finally, Paul et al. [55] already consider the computational power of quantum computing and developing a corresponding mechanism in the context of OPC UA.

5.2 Conclusion

This paper describes current industrial communication standards with relevant use cases. It covers the broad landscape of the subject through the systematic approach to literature. The findings show that OPC UA is the most mentioned standard, which can be argued to be due to its complexity and the underlying (extensible) information model. Furthermore, it can be stated that all included standards are Ethernet-based. Ethernet-based standards can run on the same infrastructure as the already existing enterprise IT infrastructure. In most cases, off-the-shelf networking components can connect the operation technology (OT) architecture to the IT architecture. This makes them very popular.

The use cases mentioned can be considered as recommendations for standard usage. Generally, OPC UA is the most suitable standard for modern production infrastructure due to its flexibility and speed of configuration. For smaller setups, MQTT is well-suited. Its topic structure makes it easy to organize information, and multiple open-source implementations on different platforms simplify customization.

A table with decisive properties of the mentioned communication standards for use in an industrial environment with a manufacturing context is summarized in Table 1.

Table 1: Overview of the mentioned standards

Criteria	***MTConnect***	***MQTT***	***OPC UA***	***Modbus TCP***	***ProfiNet***
Application Layer Protocol	HTTP	HTTP, Zigbee, etc.	HTTP, UADP, custom	custom	TCP, UDP,
Realtime capable	yes	yes	yes (config dependent)	no	yes (config dependent)
Speed	high	high	high	low	high
Information model	no	yes (by extension)	yes	no	no
Secure Communication	yes	yes	yes	yes (optional)	yes
Encoding	XML	custom	XML, custom	ASCII, custom	custom

As an outlook for future work, comparing the distribution of protocols in the literature with their actual usage in the field is interesting. Although many organizations claim industrial use of their protocols, no independent organization provides usage data.

Acknowledgments

The project "WIN4KMU" (grant number EFO 0015B-E) is funded by the Ministry of Economics, Innovation, Digitalization, and Energy of the State of North Rhine-Westphalia (MWIDE).

References

[1] Kashif, H., Khan, M.N., Awais, Q. Selection of Network Protocols for Internet of Things Applications: A Review, 359–362.

[2] Lata, N., Kumar, R. Internet of Things: A Review of Architecture and Protocols, 1027–1031.

[3] Gericke, G.A., Vermaak, H., Kurakose, R.B. Communication Protocol Review for SMART Manufacturing Units within a Cloud Manufacturing Environment, 1–6.

[4] Pliatsios, D., Sarigiannidis, P., Lagkas, T., Sarigiannidis, A.G., 2020. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. IEEE Commun. Surv. Tutorials 22 (3), 1942–1976.

[5] Gough, D., Oliver, S., Thomas, J., 2017. An introduction to systematic reviews, 2nd edition ed. Sage, Los Angeles, London, New Delhi, Singapore, Washington, DC, Melbourne, 331 pp.

[6] AMT - The Association for Manufacturing Technology. MTConnect Standard: Part 1.0 - Fundamentals.

[7] Lee, K.B., Song, E.Y., Gu, P.S., 2012. A Sensor Model for Enhancement of Manufacturing Equipment Data Interoperability. ASME International Mechanical Engineering Congress and Exposition.

[8] Malik, S., Bedillion, M.D. Event-Based Temperature Control for Machining Using MTConnect, 629–637.

[9] Edrington, B., Zhao, B., Hansel, A., Mori, M., Fujishima, M., 2014. Machine Monitoring System Based on MTConnect Technology. Procedia CIRP.

[10] ISO/IEC, 2016. Information technology — Message Queuing Telemetry Transport (MQTT) 35.100.70 Application layer.

[11] Eclipse Foundation. Sparkplug™ Specification.

[12] Salvatierra, N., 2021. Cloud Condition Monitoring Platform for Steel Rolling Mill Machines. IEEE Latin-American Conference on Communications.

[13] Ahmad, M.I., Saif, Y., Yusof, Y., Daud, M.E., Latif, K., Kadir, A.Z.A., 2022. A case study: monitoring and inspection based on IoT for milling process. Int J Adv Manuf Technol.

[14] Breunig, D.A., Schneider, M., 2019. Multi-protocol Data Aggregation and Acquisition for Distributed Control Systems. Procedia CIRP.

[15] Aliev, K., Antonelli, D., Awouda, A., Chiabert, P., 2019. Key Performance Indicators Integrating Collaborative and Mobile Robots in the Factory Networks.

[16] Bartholet, M., Überall, C., 2020. Multi-protocol bridge generation for M2M communication using MQTT. Journal of Physics: Conference Series.

[17] Yeh, C.-S.-L., 2021. Implementation of MQTT protocol based network architecture for smart factory. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture.

[18] Luchian, R.-A., Stamatescu, G., Stamatescu, I., Fagarasan, I., Popescu, D., 2021. IIoT Decentralized System Monitoring for Smart Industry Applications. 29th Mediterranean Conference on Control and Automation.

[19] IEC, 2015. OPC Unified Architecture, 1st ed. 25.040.40. doi:10.31030/2346272.

[20] VDI Verein Deutscher Ingenieure e.V., ZVEI – German Electrical and Electronic, 2015. Reference Architecture Model Industrie 4.0 (RAMI4.0).

[21] OPC Foundation. OPC 10000-2 UA Part 2: Security. https://reference.opcfoundation.org/Core/Part2/v104/docs/#4.8.

[22] OPC Foundation. OPC 10000-1: UA Part 1: Overview and Concepts: 5.2 General.

[23] OPC Foundation. OPC 10000-4: UA Part 4: Services: 4.1 Service Set model, 1st ed.

[24] OPC Foundation. OPC 30200 Commercial Kitchen Equipment. Accessed 27 July 2023.

[25] OPC Foundation. OPC 30140 Profinet. Accessed 27 July 2023.

[26] Wang, R., S.ShiZ.Meng, W., 2022. An interoperable and flat Industrial Internet of Things architecture for low latency data collection in manufacturing systems. Journal of Systems Architecture.

[27] Steininger, A., Bleicher, F., 2019. In-process monitoring and analysis of whirling motions in boring and trepanning association deep drilling. MM SCIENCE JOURNAL.

[28] Bennulf, M., Danielsson, F., Svensson, B., 2019. Identification of resources and parts in a Plug and Produce system using OPC UA. Procedia Manufacturing.

[29] Martins, A., Lucas, J., Costelha, H., Neves, C., 2021. Developing an OPC UA Server for CNC Machines. Procedia Computer Science.

[30] Kong, C., Liu, W., Niu, Q., Zhou, X., 2019. Research on Data Acquisition and Analysis of CNC Machine Tool in Smart Factory. Advances in Transdisciplinary Engineering.

[31] Cavalieri, S., Salafia, M.G., Scroppo, M.S., 2019. Integrating OPC UA with web technologies to enhance interoperability. Computer Standards & Interfaces.

[32] Park, H.M.J., 2019. OPC UA based universal edge gateway for legacy equipment. IEEE International Conference on Industrial Informatics (INDIN).

[33] Bruckner, D., Stanica, M.-P., Blair, R., Schriegel, S., Kehrer, S., Seewald, M., Sauter, T., 2019. An Introduction to OPC UA TSN for Industrial Communication Systems. Proc. IEEE 107 (6), 1121–1131.

[34] Neumann, P., Pöschmann, A., 2005. Ethernet-based real-time communications with PROFINET IO.

[35] Bogdan M. Wilamowski and J. David Irwin. The Industrial Electronics Handbook. Second Edition: Industrial Communication Systems.

[36] Duerkop, L., Trsek, H., Jasperneite, J., Wisniewski, L. Towards autoconfiguration of industrial automation systems: A case study using Profinet IO, 1–8.

[37] Dias, A.L., Sestito, G.S., Brandao, D., 2017. Performance Analysis of Profibus DP and Profinet in a Motion Control Application. J Control Autom Electr Syst 28 (1), 86–93.

[38] Ferrari, P., Flammini, A., Vitturi, S., 2006. Performance analysis of PROFINET networks. Computer Standards & Interfaces 28 (4), 369–385.

[39] Ionescu, D., Filipescu, A., Simion, G., Mincă, E., Cernega, D., Şolea, R., Filipescu, A., 2022. Communication and Control of an Assembly, Disassembly and Repair Flexible Manufacturing Technology on a Mechatronics Line Assisted by an Autonomous Robotic System. Inventions 7 (2), 43.

[40] Dias, A.L., Turcato, A.C., Sestito, G.S., Brandao, D., Nicoletti, R., 2021. A cloud-based condition monitoring system for fault detection in rotating machines using PROFINET process data. Computers in Industry 126, 103394.

[41] Modbus Organization Inc., 2012. Modbus Application Protocol Specification, 1st ed.

[42] Zheng, Y. An active transmission ModBus protocol based on Zigbee.

[43] Zhang, B., Hu, S. Design and Implementation of Intelligent Acquisition Terminal Based on Modbus.

[44] Chattha, H.A., G.KhanA. Q.Abid, M., 2021. Implementation of Cyber-Physical Systems with Modbus Communication for Security Studies. 2021 International Conference on Cyber Warfare and Security, ICCWS 2021 - Proceedings.

[45] Modbus Organization Inc., 24.10.06. MODBUS Messaging on TCP/IP Implementation Guide, 1st ed.

[46] Jingran, W., Mingzhe, L., Aidong, X., Bo, H., Xiaojia, H., Xiufang, Z., 2020. Research and Implementation of Secure Industrial Communication Protocols. Proceedings of 2020 IEEE International Conference on Artificial Intelligence and Information Systems, ICAIIS 2020.

[47] Pliatsios, D., 2020. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. IEEE Communications Surveys and Tutorials.

[48] Mourtzis, D., 2019. Mapping vulnerabilities in the industrial internet of things landscape. Procedia CIRP.

[49] Boppana, T.K., 2022. Security risks in MQTT-based Industrial IoT Applications. 2022 IEEE International Conference on Omni-Layer Intelligent Systems, COINS 2022.

[50] Rajesh, L., 2020. Security vulnerabilities of scada communication protocols. International Journal of Scientific and Technology Research.

[51] Bienhaus, D., Jäger, L., Rieke, R., Krauß, C., 2020. Gateway for Industrial Cyber-Physical Systems with Hardware-Based Trust Anchors.

[52] Dinculeană, D., Cheng, X., 2019. Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. Applied Sciences.

[53] Kant, D., 2021. Analysis of IoT security risks based on the exposure of the MQTT Protocol. IS and T International Symposium on Electronic Imaging Science and Technology.

[54] Kohnhauser, F., Meier, D., Patzer, F., Finster, S., 2021. On the Security of IIoT Deployments: An Investigation of Secure Provisioning Solutions for OPC UA. IEEE Access.

[55] Paul, S., 2020. Hybrid OPC UA: Enabling Post-Quantum Security for the Industrial Internet of Things. IEEE International Conference on Emerging Technologies and Factory Automation.

Biographies

Furkan Ercan (*1992) is a scientific associate at the Chair of Production Systems (LPS) at the Ruhr-Universität Bochum. His research interests include Industry 4.0, simulation, production planning, and machine learning.

Maximilian Bega (*1995) is a scientific associate at the Chair of Production Systems (LPS) at the Ruhr-Universität Bochum. His research interests include Industry 4.0, IT security, machining, and resilient production systems.

Bernd Kuhlenkötter (*1971) was responsible for product management and technology at ABB Robotics Germany until 2009. In 2009, Bernd Kuhlenkötter took over the professorship for "Industrial Robotics and Production Automation" at the Technical University of Dortmund. Univ. Prof. Dr.-Ing. Bernd Kuhlenkötter has held the professorship for "Production Systems" at the Ruhr University Bochum since 2015.