

Evaluation of OPC-UA communication in an autonomous advanced manufacturing cell implementation

Avaliação da comunicação OPC UA em uma implementação de célula autônoma de manufatura avançada

Rodrigo Filev Maia¹ , Ângelo Jorge Bálamo² , Guilherme Alberto Wachs Lopes¹ , Alexandre Augusto Massote³ , Fábio Lima³ 

¹Centro Universitário FEI, Departamento de Ciência da Computação, Bernardo do Campo, SP, Brasil. E-mails: rfilev@fei.edu.br; gwachs@fei.edu.br

²Centro Universitário FEI, Departamento de Engenharia Elétrica, Bernardo do Campo, SP, Brasil. E-mail: angeloj.balsamo@live.com

³Centro Universitário FEI, Departamento de Engenharia de Produção, Bernardo do Campo, SP, Brasil. E-mails: massote@fei.edu.br; flima@fei.edu.br

How to cite: Maia, R. F., Bálamo, A. J., Lopes, G. A. W., Massote, A. A., & Lima, F. (2020). Evaluation of OPC-UA communication in an autonomous advanced manufacturing cell implementation. *Gestão & Produção*, 27(4), e5414. <https://doi.org/10.1590/0104-530X5414-20>

Abstract: The recent development of advanced manufacturing concepts brings new challenges for developing countries in order to prepare their workforce and industries for local and global markets. To explore and disseminate advanced manufacturing concepts, the first autonomous advanced manufacturing cell developed in Brazil as a result of a partnership between global and local companies and academia was designed and evaluated. This paper aims to describe the advanced manufacturing cell, the equipment composing the infrastructure, and the network topology and equipment that could deal with the heterogeneity of equipment and protocol. Moreover, the behavior of the Open Platform Communications Unified Architecture (OPC UA) communication framework (and related protocols) as the integration element between the equipment composing the cell was evaluated. The results indicated that the OPC UA communication framework promotes a low traffic overhead and can also be used to carry data from the traditional protocols in their fields without restrictions that could hinder production. The paper also discusses how the exchange of data occurred between the equipment used in the production and the control systems via the protocol studied. The OPC UA communication framework protocols presented a messaging structure and data transport characteristics that satisfy the integration needs between equipment of several manufacturers that composed an autonomous cell of advanced manufacturing. This paper also presents some key challenges to integrating all equipment not addressed by the OPC UA reference model.

Keywords: OPC UA; System integration; Network analysis; Industry 4.0.

Resumo: O recente desenvolvimento de conceitos de manufatura avançada traz novos desafios para os países em desenvolvimento, a fim de preparar sua força de trabalho e indústrias para os mercados locais e globais. Para explorar e disseminar os conceitos de manufatura avançada, projetou-se e avaliou-se a primeira célula de manufatura avançada autônoma desenvolvida no

Brasil a partir da parceria entre empresas globais e locais e a academia. Este trabalho tem como objetivo descrever a célula de manufatura avançada, os equipamentos que compõem a infraestrutura, a topologia de rede e os equipamentos que poderiam lidar com a heterogeneidade de equipamentos e protocolos. Além disso, o comportamento da estrutura de comunicação do OPC UA (e protocolos relacionados) como o elemento de integração entre os equipamentos que compõe a célula é avaliado. Os resultados indicaram que a estrutura de comunicação do OPC UA promove uma baixa sobrecarga de tráfego, bem como pode ser usada para transportar dados dos protocolos tradicionais em seus campos sem restrições que possam prejudicar a produção. O artigo também discute como ocorreu a troca de dados entre os equipamentos utilizados na produção e os sistemas de controle através do protocolo estudado. Os protocolos da estrutura de comunicação OPC UA apresentaram uma estrutura de mensagens e características de transporte de dados que satisfazem as necessidades de integração entre equipamentos de diversos fabricantes que compunham a célula autônoma de manufatura avançada. Este documento também apresenta alguns desafios fundamentais para integrar todos os equipamentos não abordados pelo modelo de referência OPC UA.

Palavras-chave: OPC UA; Integração de sistemas; Análise de rede; Indústria 4.0.

1 Introduction

Industrial development has been evolving broadly and rapidly by adopting new information technologies in order to promote more dynamic and adaptable production systems. According to Schwab (2016), this trend is part of the fourth industrial revolution, with technological innovations in several segments, interacting in the physical, digital, and biological domains, which has implications for all sectors of society, such as health, communication, energy, and production, among others. The physical, digital, and biological domains are deeply related and are grouped into megatrends. Schwab (2016) also stated that all new developments and technologies have one key feature in common: they take advantage of the power of digitization and information technology.

In the effort to develop the concepts and technologies related to the fourth industrial revolution, industry and academia are working in association on key concepts such as the Internet of Things (IoT) and Cybernetic Systems, and since 2014 there has been an increase in the volume of academic research related specifically to the theme of Industry 4.0, with increasing demand for the requisite knowledge of the emergent technologies related to the theme (Kang et al., 2016).

Governmental and non-governmental organizations are working to ensure that the development of the Industry 4.0 theme is guided by standards and recommendations such as the Reference Architecture Model for Industry 4.0 (RAMI), Report 4.0 of the German Association of Engineers, the Technical and Scientific Association for Electrical, Electronic and Information Technology (VDI/VDE-GMA Society for Measurement and Automatic Control, 2015), and the Association of Electrical and Electronic Manufacturers of Germany (ZVEI), the report of recommendations for the implementation of the strategic initiative of Industry 4.0 of the National Academy of Science and Engineering of Germany (Acatech, 2013), and the report from the Industrial Internet Consortium (IIC) (IIC, 2015), a nonprofit consortium of industry, government, and academia for the United States Internet industry with a reference architecture model for the industrial Internet, and other initiatives in countries where there is interest in deployment of the model.

Several studies are under development to apply OPC UA as an integration mechanism to Industry 4.0 manufacturing cells (or advanced manufacturing cells).

Zeulka et al. (2018) present typical communication activities on the Industry 4.0 platform and compare Internet communication network protocols to OPC UA as an element of interoperation between different equipment and time sensing applications. Schlechtendahl et al. (2015) discuss the use of gateways to adapt existing industrial infrastructures to Industry 4.0. In this present work, the same concept is applied using an industrial PC (IPC) as the gateway to convert legacy system communication mechanisms into OPC UA. The application of OPC UA in an Industry 4.0 scenario is presented by Veichtlbauer et al. (2017), providing some quantitative metrics of the application of OPC UA. This present work discusses the performance of the OPC UA in a fully automated process and also the issues related to interoperation between a multitude of equipment branches. The use of OPC UA with open hardware (Arduino) to control a 3D printer is discussed in Müller et al. (2017), in which some OPC UA communication properties are explored, and this work contributes by exploring the same mechanisms in a manufacturing cell with the same equipment applied in the industries. Profanter et al. (2019) compare the performance of several Internet de facto standard protocols such as JSON and MQTT with OPC UA in a computational environment in which the CPU and memory load were measured for a number of controlled nodes.

This work discusses the application of Industry 4.0 concepts and the use of OPC UA in an advanced manufacturing cell. The proposal was to develop an Industry 4.0 demonstrator to highlight the benefits of this new concept. Several enterprises, technology providers, and universities worked together on a collaborative project, in which they all provided equipment and technical expertise to develop the system architecture and technology integration between several brands of equipment. Such heterogeneity demanded an interoperation mechanism and that was the primary role of the OPC UA. According to the OPC Foundation: “OPC UA is a platform-independent standard through which various kinds of systems and devices can communicate by sending request and response Messages between Clients and Servers or NetworkMessages between Publishers and Subscribers over various types of networks”. The OPC UA features allowed interoperation in a heterogeneous environment, providing a robust and reliable message exchange mechanism and parameter definition to define and control all processes in all equipment from the advanced manufacturing cell.

2 Literature review

In the next subsections, the key definitions and concepts related to the system architecture and integration applied in the advanced manufacturing cell are presented, with a particular focus on Industry 4.0 and communication technologies applied in manufacturing systems.

2.1 Industry 4.0

Used for the first time at the Hanover Fair in 2011, the term “Industry 4.0” refers to the fourth industrial revolution and is often understood to be the application of the generic concept of cyber-physical systems (CPSs) to industrial production systems (cyber-physical production systems) (Drath & Horch, 2014; Perez et al., 2015; Jiang, 2017; Jazdi, 2014). The use of CPSs can provide, for example, a combined approach between the process and the product in automated production systems, as proposed in Vogel-Heuser et al. (2017).

From the academic side, an increase in the number of works on the subject of I4.0 has been observed from 2014 (Kang et al., 2016), leaving the hype behind (Drath & Horch, 2014). The researches encompass all the components and technologies of I4.0 considering the discussion of concepts and implementation. Trotta & Garengo (2018) apply a bibliometric methodology to identify common terms in 618 selected papers in order to establish a term understanding related to Industry 4.0 (and used in this work).

Kalor et al. (2018) first proposed a hierarchical architecture of the smart factory and then analyzed the key technologies in relation to the physical resource layer, the network layer, and the data application layer.

Sisinni et al. (2018) clarify the concepts of the IoT, the Industrial IoT, and Industry 4.0. They highlight the opportunities brought in by this paradigm shift as well as the challenges for its realization. In particular, they focus on the challenges associated with the need for energy efficiency, real-time performance, coexistence, interoperability, and security and privacy. They also provide a systematic overview of the state-of-the-art research efforts and potential research directions to solve Industrial IoT challenges.

The work of Lu (2017) provides a literature overview of Industry 4.0, stressing the necessity of interoperability in this new manufacturing model.

2.2 Communication in Industry 4.0 – OPC UA

Wang et al. (2017) present a cloud-centric framework for the implementation of the smart factory. Three protocols are used in the implementation: Ether-CAT, DDS, and OPC UA, but OPC UA is only used to send data to the cloud.

Zarte et al. (2016) describe the building of an Industry 4.0 compliant lab environment, which consists of a service-oriented shop floor (OT level) and three major management systems: an ERP system, a database, and simulation for predictive maintenance (IT level). The OPC UA protocol is used in the integration of lower-level systems and upper-level systems.

Godoy & Perez (2016) present a solution to enhance the connectivity of a legacy Flexible Manufacturing System (FMS), which constitutes the first step in the adoption of the Industry 4.0 concept. The idea is to provide the retrofit of a classical FMS to insert this kind of system into the Industry 4.0 world through the adoption of modern sensors.

In Pedone & Mezgar (2018), after a brief introduction to cloud criticality and cloud-based manufacturing, the mutual conceptual similarities in modeling distributed industrial services of two of the major standardization frameworks for industrial Internet architectures are presented: the Industrial Internet Reference Architecture (IIRA) and the Reference Architectural Model Industry (RAMI 4.0). Both indicate OPC UA as a strategic player in the realization of industrial services interoperability.

Kalor et al. (2018) present methods of slicing deterministic and packet-switched industrial communication protocols which simplify the manageability of heterogeneous networks with various application requirements.

Tang et al. (2018) present an architecture of a smart shop floor based on physical, logical, and communication layers that embed intelligent approaches within manufacturing processes. Every physical entity on the smart shop floor is regarded as an autonomous intelligent logical unit that performs operations guided by distributed control functions. Moreover, computing power and optimization approaches are embedded into each logical unit to make decisions to respond agilely to the frequent occurrences of unexpected disturbances on the shop floor.

Jirkovsky et al. (2018) describe the issues related to integration and propose a plug-and-play solution that allows a self-describing device producing self-described data to be plugged into a larger system. This solution utilizes OPC UA and Semantic Web technologies to achieve integration at various levels.

Terzimehic et al. (2017) present the design of Industry 4.0 compliant control software architecture resulting from an iterative design process. The architecture is based on the reconfiguration services of the IEC 61499 standard and service orchestration via OPC UA. They demonstrate the software architecture's compliance with Industry 4.0 requirements on an aluminum cold rolling mill plant demonstrator.

Hoffmann et al. (2016) propose an architectural approach for a Multi-Agent System that is based on OPC UA as a modeling interface and as a semantic approach for the integration of agent-based systems into existing manufacturing sites. For this purpose, they define a domain ontology for the representation of intelligent software agents and for the mapping of an agent-based communication by making use of the OPC UA meta-model.

The main goal of the work of Garcia et al. (2016) is to make vertical integration a reality by means of a low-cost CPPS architecture that provides access to process data. The paper describes both the hardware platform as well as the software, including the proposed configuration file of the OPC UA server.

Wan et al. (2018) present an information exchange model based on object linking for process control unified architecture (OPC UA), software-defined industrial networking (SDIN), and device-to-device (D2D) communication technology is proposed. Furthermore, ontology modeling is proposed and a multi-agent technology is employed to achieve dynamic resource management.

3 Methodology

The present work is quantitative and exploratory in terms of the research methodology. The work is based on the implementation of an advanced manufacturing cell as a demonstrator of the concepts of Industry 4.0. The construction of the demonstrator is organized by ABIMAQ (Brazilian Association of the Machines Manufacturers). ABIMAQ invites member companies and educational institutions to participate in the demonstrator project, generating the necessary collaborative work for the development of Industry 4.0. Companies provide the equipment and manpower for implementation and educational institutions provide students, professors, and researchers to work on the project. In this work, the communication of several pieces of equipment with different communication protocols was implemented in the advanced manufacturing cell, using convergence to the OPC-UA protocol through industrial computers. The performance of the communication system based on this protocol was then deeply analyzed through data collection during three days of operation of the cell. Considering the presented literature review on Industry 4.0 and specifically on the OPC UA protocol, this work contributes to the subject of OPC UA because it presents and evaluates the use of the protocol and the communication data in an Industry 4.0 demonstrator that effectively produces a customized product. The communication data among machines on the lower level and the communication to the higher level, considering vertical integration, are presented. In the proposed demonstrator, there are the core elements of Industry 4.0 advanced manufacturing cells, each belonging to a different company with its own technology, and it is important to evaluate how OPC UA is able to deal with heterogeneous technologies effectively using an IPC as an interface between industrial and proprietary protocols and OPC UA as well as how OPC UA can deal with heterogeneous data.

4 The proposed advanced manufacturing cell

The design of a manufacturing cell considering several Industry 4.0 concepts was proposed by ABIMAQ (Brazilian Association of the Machines Manufacturers). The proposal consisted in gathering manufacturers, universities, technology providers, and startups, among others, in a collaborative project. The manufacturing demonstrator was presented at a Brazilian Machinery and Tools fair in São Paulo, Brazil, in May 2017.

The first step of the project was to determine the product that would be produced by the cell. After several meetings and discussions, a mobile phone holder (MPH) with a mechanical sound amplifier was chosen. One of the concepts of Industry 4.0 is the mass production of customized products. Considering that, the MPH was designed to have three different customizations: adjustment of the dimensions to fit the customer's mobile, the choice of one color among three available ones, and a personalized text to be printed on the MPH.

The project was virtually commissioned using digital manufacturing software tools and has autonomous production modules, machine-to-machine communication, big data, data analytics, and augmented reality, among other Industry 4.0 concepts.

Figure 1 presents the Industry 4.0 demonstrator and its modules. In the following, a short description of each module is presented. The description of the modules is as follows:



Figure 1. Industry 4.0 demonstrator and its modules.

1. Milling module: composed of one robot, two milling machines (three and five axes), 30-position storage with three different color blanks, and a transfer cell. The management of the resources of this module is performed by the module itself;
2. Welding module: composed of a store of metal sheets and an automatic welding cell;
3. Input module: where the customer can select the product features (customize the product). After the customization is completed by the client, a production demand is created to the line with integration with the ERP (Enterprise Resource Planning), MES (Manufacturing Execution System), and PLM (Product Lifecycle Management) software. In this module, it is also possible to scan the dimensions of the customer's mobile, providing important customization of the product;
4. Recording module: composed of two robots and two different recording methods. The module can choose the recording method (laser or micro-dots);
5. Assembly module: composed of a pneumatic manipulator that integrates two parts of the product mechanically using RFID codes presented in the components as reference;

- 6. Delivery module: composed of a collaborative robot, a delivery buffer, and an output totem. The product waits until its retirement from the customer, interacting with the collaborative robot.

All modules have industrial PC control panels, managing the safety and production conditions locally.

4.1 Network topology of the advanced manufacturing cell

Figure 2 depicts the network topology used in the manufacturing cell. Although the OPC UA is the communication data structure between all modules of the manufacturing cell and PLM, ERP, and MES operate using OPC UA natively, several types of industrial equipment operate with other industrial protocols. To perform the network protocol conversion, an IPC provides the communication interface of each production module and executes an OPC UA server software application that controls the communication process with MES and translates OPC UA to the industrial protocol used inside the production module.

The advanced manufacturing cell runs with a multitude of protocols such as Profibus, ProfiNet, and Ethernet/IP. The conversion pattern is depicted in Figure 3. Such a protocol communication conversion mechanism is useful in a situation where a machine without OPC UA support is already installed in a factory and would be part of a manufacturing cell using the OPC UA communication mechanism. This is a typical situation in the Brazilian industrial scenario.

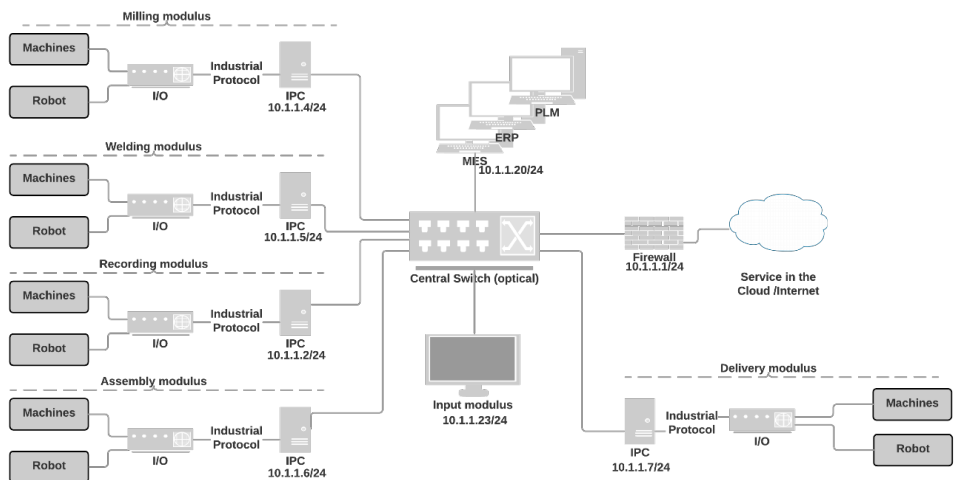


Figure 2. Industry 4.0 demonstrator and its modules (I/O: input/output).

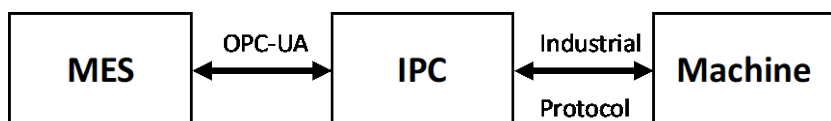


Figure 3. Communication between MES and the production cell.

5 Performance and characterization of an OPC UA message stream

In order to evaluate the infrastructure behavior of the advanced manufacturing cell, all network packets that crossed the central switch (Figure 2) were copied to a single interface (port mirroring), where a computer running a network protocol analyzer was connected. The network star topology makes all traffic pass through this single piece of equipment. This strategy provided robustness, the network connections between equipment were independent, which simplified the management and troubleshooting issues, and the optical switch in the center of the topology made it possible to copy all traffic from all interfaces to a single high-speed interface. Both the switch network interface and computer interface used by the protocol analyzer had more traffic-processing capacity than the peak traffic observed in the advanced manufacturing cell (without oversubscription). The topology network also had traffic segmentation through Virtual LAN (VLAN) technology to avoid situations in which incorrect behavior by equipment would flood the network with broadcasts or other types of undesirable traffic. At least one piece of equipment had a default network protocol, not OPC UA, that generated broadcasts in the network, and by using a star topology such broadcast traffic was filtered without overloading the links from the other equipment. There was no data loss during the capturing process.

The OPC UA communication schema followed the Client-Server model with several concurrent communication sessions between equipment. All equipment worked as Combined OPC UA Server and Client (OPC Foundation, 2017). Each piece of equipment operated as a client when sending messages to the servers or other equipment in the line and at the same time operated as the server while each piece of equipment was able to receive command and messages from other equipment in the line. Such situations occurred to synchronize activities since each product customization required variable production time. All equipment and messages followed the AddressSpace model (OPC Foundation, 2017) to describe attributes and data types of each equipment parameter, all messages were exchanged using OPC UA TCP, and the data payload was coded in XML/text and JSON format. All communication between equipment in the manufacturing cell and the cloud services was protected by a Next-Generation Firewall. The establishment of an OPC UA communication channel between two devices passes through a sequence of events. According to Mahnke et al. (2009), the first step is the establishment of a channel (OpenSecureChannel), which is followed by the establishment of a security mechanism with identification of the communication elements and controls over the message sequencing (SecureChannel). Only after the creation of the OPC UA communication channel can other messages and services be exchanged between the elements of a cell, such as the GetEndpoints Service, which is responsible for obtaining descriptions about an element of a particular equipment.

Figure 4 depicts several types of packets exchanged in OPC UA data streams between equipment which composes the manufacturing cell and the MES (IP address 10.1.1.20). The communication starts with the three-way handshake of the TCP protocol (like any standard TCP communication) initiated by the MES server to connect with an equipment in the manufacturing cell to the IPC. After the three-way handshake, the OPC UA messages start, and the MES server (Figure 5) sends an OPC UA Hello message (58 bytes), where data about the buffer size for receiving message and other information are exchanged, such as the server identification (address and TCP port) that will be used (OPC.TCP://cel Entrega: 4840).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.20	10.1.1.6	OpcUa	144	UA Secure Conversation Message: RegisterNodesRequest
2	0.025975	10.1.1.6	10.1.1.20	OpcUa	114	UA Secure Conversation Message: RegisterNodesResponse
3	0.026225	10.1.1.20	10.1.1.6	OpcUa	201	UA Secure Conversation Message: ReadRequest
4	0.056000	10.1.1.6	10.1.1.20	OpcUa	136	UA Secure Conversation Message: ReadResponse
5	0.069999	10.1.1.20	10.1.1.6	OpcUa	183	UA Secure Conversation Message: ReadRequest
6	0.095979	10.1.1.6	10.1.1.20	OpcUa	129	UA Secure Conversation Message: ReadResponse
7	0.109987	10.1.1.20	10.1.1.6	OpcUa	121	UA Secure Conversation Message: UnregisterNodesRequest
8	0.135980	10.1.1.6	10.1.1.20	OpcUa	106	UA Secure Conversation Message: UnregisterNodesResponse
9	0.158851	10.1.1.4	10.1.1.106	OpcUa	194	UA Secure Conversation Message: PublishResponse
10	0.159997	10.1.1.20	10.1.1.6	OpcUa	144	UA Secure Conversation Message: RegisterNodesRequest
11	0.186013	10.1.1.6	10.1.1.20	OpcUa	114	UA Secure Conversation Message: RegisterNodesResponse
12	0.186014	10.1.1.20	10.1.1.6	OpcUa	201	UA Secure Conversation Message: ReadRequest
13	0.208432	10.1.1.106	10.1.1.4	OpcUa	125	UA Secure Conversation Message: PublishRequest

Figure 4. OPC UA message exchange between MES and production module.

The Hello message is succeeded by an Acknowledgment message of 82 bytes (Figure 5). Once the message is recognized, the IPC starts a SecureChannel (OpenSecureChannelRequest) with the MES server (Figure 6), where a sequence number for subsequent OPC UA messages and the RequestID are defined. This message is not defined as the SecureChannelID yet (value 0); this will only be defined in the answer OpenSecureChannelResponse (value 20302 in Figure 7). The SecureChannelID value will be used in all other messages belonging to this communication stream. In the message GetEndPointRequests, the description of the device is requested, while the message GetEndPointResponse sends the answer to the request (Figure 8) in several segments, which indicates that OPC-UA messages will be bigger than 1480 bytes, that is, the default payload size or maximum transfer unit (MTU) of an Ethernet network. It is important to note that the response message has a size of 4755 bytes and that message is segmented into several TCP packets (not identified as the OPC UA protocol because the packets identified as TCP only do not have the OPC UA header). The protocol analyzer places the OPC UA message as the last captured package, although the analysis of the TCP protocol (message highlighted as a link) indicates that the packet with OPC UA is the first and is followed by the other network packets (as expected).

No.	Time	Source	Destination	Protocol	Length	Info
44	0.025854	10.1.1.6	10.1.1.20	opcua	136	UA Secure Conversation message: ReadResponse
78	0.045453	10.1.1.20	10.1.1.6	OpcUa	183	UA Secure Conversation Message: ReadRequest
89	0.046979	10.1.1.20	10.1.1.7	OpcUa	112	Hello message
90	0.047880	10.1.1.7	10.1.1.20	OpcUa	82	Acknowledge message
91	0.047881	10.1.1.20	10.1.1.7	OpcUa	187	OpenSecureChannel message: OpenSecureChannelRequest
95	0.048830	10.1.1.7	10.1.1.20	OpcUa	190	OpenSecureChannel message: OpenSecureChannelResponse

▶ Frame 89: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
 ▶ Ethernet II, Src: Beckhoff_15:e9:47 (08:01:05:15:e9:47), Dst: Beckhoff_1b:93:0e (08:01:05:1b:93:0e)
 ▶ Internet Protocol Version 4, Src: 10.1.1.20, Dst: 10.1.1.7
 ▶ Transmission Control Protocol, Src Port: 54064, Dst Port: 4840, Seq: 1, Ack: 1, Len: 58
 ▼ OpcUa Binary Protocol
 Message Type: HEL
 Chunk Type: F
 Message Size: 58
 Version: 0
 ReceiveBufferSize: 65536
 SendBufferSize: 65536
 MaxMessageSize: 16777216
 MaxChunkCount: 5000
 EndpointUrl: opc.tcp://CeI_Entrega:4840

Figure 5. OPC UA Hello message details.

Another communication stream is evaluated between the 10.1.1.6 equipment (Assembly module) and 10.1.1.20 (MES). The sequence of messages depicted in Figure 5 shows the MES server sending and receiving commands and messages indicating the status of the Assembly module.

According to Mahnke et al. (2009), the Service RegisterNode has the function of providing a safe channel between elements. This bridge communication is controlled by a NodeID identifier. The Read message type requests and carries all values to be

exchanged, allowing the client to receive the requested information from the server. The UnregisterNode finishes the communication channel.

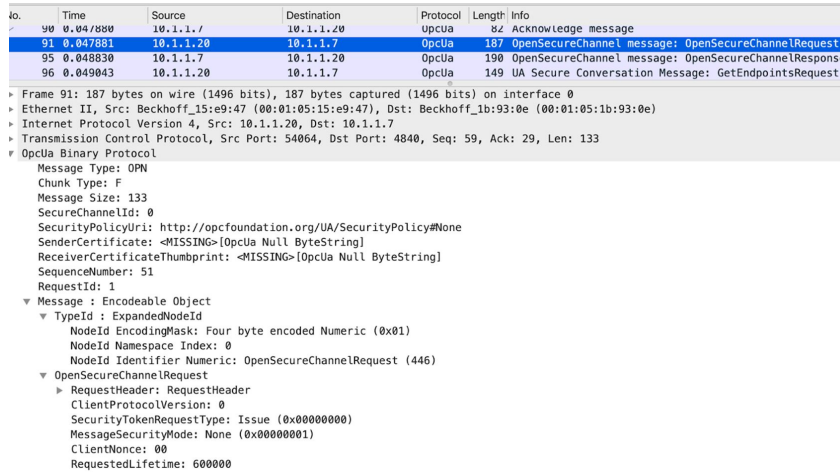


Figure 6. OPC UA SecureChannel details.

All messages exchanged between the Assembly module and the MES server belong to the same SecureChannelID (14543) and the same SecurityTokenID (2), and the SecuritySeqNumber and SecurityRequestID codes follow an incremental sequence (Table 1). When a new RegisterNodeRequest message is sent, both the Security Sequence Number and the Security Request ID keep the same sequence number.

5.1 Network performance

The total number of packets per second transmitted in the manufacturing cell is presented in Figure 9. During the manufacturing cell operation, several types of messages were exchanged between machines, such as layer 2 protocols to network or IPC control, messages from the operating system, and messages from the Input module. In this network traffic analysis, there is no traffic using other industrial protocols except for OPC UA.

Table 1. OPC UA sequence numbers – control of communication channel.

	SecureChannelID	SecurityTokenID	Sec. Seq. Num.	Sec. Request ID
RegisterNodeReq.	14543	2	78237	78187
RegisterNodeResp.	14543	2	78237	78187
ReadRequest.	14543	2	78238	78188
ReadResponse.	14543	2	78238	78188
ReadRequest.	14543	2	78239	78189
ReadResponse.	14543	2	78239	78189
UnregisterNodeReq.	14543	2	78240	78190
UnregisterNodeResp.	14543	2	78240	78190
RegisterNodeReq.	14543	2	78241	78191

There is more data exchange during starting of the manufacturing cell than during regular operation. During the operation time, a data exchange rate of about 1750 packets per second can be observed.

Time	Source	Destination	Protocol	Length	Info
91	0.047881	10.1.1.20	10.1.1.7	OpcUa	187 OpenSecureChannel message: OpenSecureChannelRequest
95	0.048830	10.1.1.7	10.1.1.20	OpcUa	190 OpenSecureChannel message: OpenSecureChannelResponse
96	0.049043	10.1.1.20	10.1.1.7	OpcUa	149 UA Secure Conversation Message: GetEndpointsRequest
104	0.050166	10.1.1.7	10.1.1.20	OpcUa	429 UA Secure Conversation Message: GetEndpointsResponse

▶ Frame 95: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
 ▶ Ethernet II, Src: Beckhoff_1b:93:0e (00:01:05:1b:93:0e), Dst: Beckhoff_15:e9:47 (00:01:05:15:e9:47)
 ▶ Internet Protocol Version 4, Src: 10.1.1.7, Dst: 10.1.1.20
 ▶ Transmission Control Protocol, Src Port: 4840, Dst Port: 54064, Seq: 29, Ack: 192, Len: 136
 ▼ OpcUa Binary Protocol
 Message Type: OPN
 Chunk Type: F
 Message Size: 136
SecureChannelId: 20302
 SecurityPolicyUri: http://opcfoundation.org/UA/SecurityPolicy#None
 SenderCertificate: <MISSING>[OpcUa Null ByteString]
 ReceiverCertificateThumbprint: <MISSING>[OpcUa Null ByteString]
 SequenceNumber: 51
 RequestId: 1
 ▼ Message : Encodable Object
 ▼ TypeId : ExpandedNodeId
 NodeId EncodingMask: Four byte encoded Numeric (0x01)
 NodeId Namespace Index: 0
 NodeId Identifier Numeric: OpenSecureChannelResponse (449)
 ▶ OpenSecureChannelResponse

Figure 7. OPC UA SecureChannelID number definition.

No.	Time	Source	Destination	Protocol	Length	Info
100	0.050053	10.1.1.7	10.1.1.20	TCP	1514	4840 → 54064 [ACK] Seq=165 Ack=287 Win=33294 Len=1460 [TCP segment of a reassembled PDU]
101	0.050054	10.1.1.7	10.1.1.20	TCP	1514	4840 → 54064 [ACK] Seq=1625 Ack=287 Win=33294 Len=1460 [TCP segment of a reassembled PDU]
102	0.050163	10.1.1.20	10.1.1.7	TCP	60	54064 → 4840 [ACK] Seq=287 Ack=3085 Win=65536 Len=0
103	0.050165	10.1.1.7	10.1.1.20	TCP	1514	4840 → 54064 [ACK] Seq=3085 Ack=287 Win=33294 Len=1460 [TCP segment of a reassembled PDU]
104	0.050166	10.1.1.7	10.1.1.20	OpcUa	429	UA Secure Conversation Message: GetEndpointsResponse
105	0.050396	10.1.1.20	10.1.1.7	TCP	60	54064 → 4840 [ACK] Seq=287 Ack=4920 Win=65536 Len=0
106	0.050397	10.1.1.20	10.1.1.7	OpcUa	111	CloseSecureChannel message: CloseSecureChannelRequest

Figure 8. OPC UA message in several PDUs (Protocol Data Units).

An error rate of about 10% of network traffic was detected (the lower line in Figure 9). A detailed analysis indicates that all error packets are related to one native service running in the IPC that had no influence in the manufacturing cell operation but was activated during the experiments.

Taking into consideration the total network traffic and the packet size distribution, 99.65% of packets are small packets of up to 639 bytes (Table 2), which indicates a fragmented traffic since most transmitted packets are less than one-third of the maximum packet size in an IP network [considering 1500 bytes of maximum transfer units (MTUs of a standard Ethernet network)].

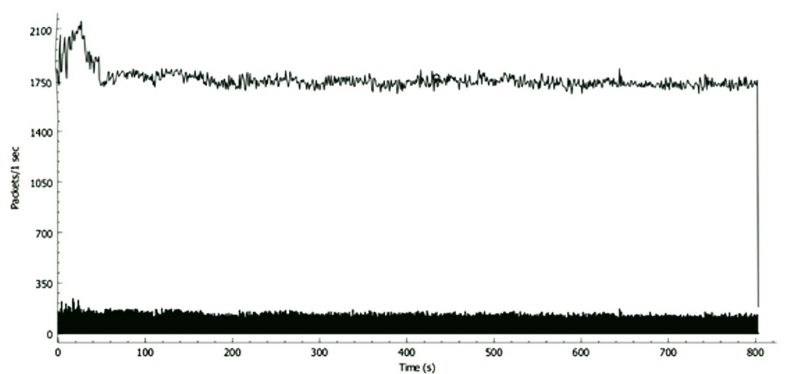


Figure 9. Total package exchange in the manufacturing cell.

The TCP traffic represents 31% of all traffic (Table 3) of the manufacturing cell. Most TCP traffic (98.49%) has a packet size of up to 639 bytes, and 85.59% of this traffic has a packet size of up to 159 bytes. Taking into consideration the size of the IP and TCP headers (20 bytes each), the payload size is up to three times greater than the headers for most traffic. The TCP traffic is also segmented traffic in this network.

Table 2. Distribution of packet sizes of all network traffic.

Packet Lengths	Count	Average	Min. value	Max. value	Rate (ms)	Percentage
0-19	0	---	---	---	---	---
20-39	0	---	---	---	---	---
40-79	1043348	60	42	79	1.2991	73.98%
80-159	299473	114.38	80	159	0.3729	21.23%
160-319	28669	207.81	161	318	0.0357	2.03%
320-639	32190	439.06	321	625	0.0401	2.28%
640-1279	1578	731.44	655	1259	0.0020	0.11%
1280-2559	5046	1513.87	1348	1514	0.0063	0.36%

Table 3. Distribution of packet size of all TCP traffic in the manufacturing cell network.

Packet Lengths	Count	Average	Min. val.	Max. value	Rate (ms)	Percentage
0-19	0	---	---	---	---	---
20-39	0	---	---	---	---	---
40-79	78254	59.92	54	78	0.0974	17.89%
80-159	296068	114.58	81	159	0.3686	67.70%
160-319	26978	206.43	161	318	0.0336	6.17%
320-639	29399	446.17	325	625	0.0336	6.72%
640-1279	1575	731.19	655	1259	0.0020	0.36%
1280-2559	5045	1513.89	1348	1514	0.0063	1.15%

The OPC UA traffic (Table 4) represents 11.10% of all TCP traffic in the manufacturing cell. All other TCP traffic is related to software related the user interface of the Input module, MES, and ERP traffic, which is part of the useful traffic of the manufacturing cell. The payload of the OPC UA messages varies from 80 up to 319 bytes.

This is an expected payload because most of this traffic is composed of the commands sent to the production modules and their respective replies. Even considering data related to product customization, the packet sizes should be small since such data is composed of the color of the body of the MPH made by a resin block (integer – 4 bytes), the smartphone dimensions (three dimensions – integer – 12 bytes), and a message composed of up to 20 characters (20 bytes).

Figure 10 depicts the OPC UA traffic across the advanced manufacturing cell. An oscillatory pattern in which traffic flow varies from a minimum transmission peak of approximately 55 packets per second to a maximum peak of approximately 72 packages per second can be observed.

According to the acquired data (Figure 11), the communication between the Delivery module and MES exchanged the largest number of packages, which is a consequence of the number of operations involved in this activity. In the Delivery module, the consumer took this product directly from a collaborative robot, an operation which involves the Delivery module reading a QR code that represents the consumer order and sending this information to ERP, the search for the product in the stock (OPC UA messages), and the set of commands telling the robot to take the product and deliver it directly to the consumer (also OPC UA messages).

Table 4. Distribution of packet size of all OPC UA traffic in the manufacturing cell network.

Packet Lengths	Count	Average	Min. val.	Max. value	Rate (ms)	Percentage
0-19	0	---	---	---	---	---
20-39	0	---	---	---	---	---
40-79	38066	127.41	106	151	0.0474	78.36%
80-159	10514	192.18	183	294	0.0131	21.64%

The Milling module was the second module with more data exchanged as a consequence of two factors: (i) the number of variables assigned to this module and (ii) the number of processes involved in this module, such as the use of a robot that takes the resin block from a magazine and puts it in more than one milling machine.

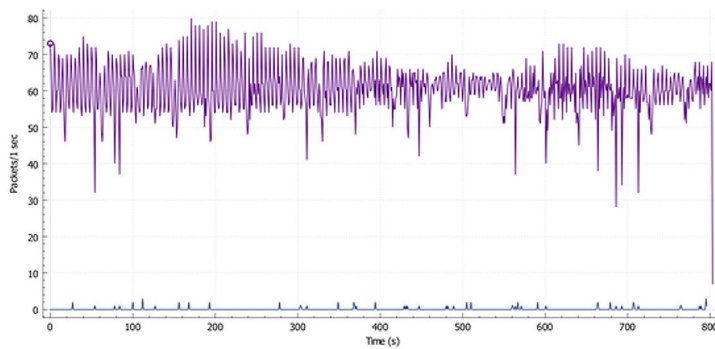


Figure 10. OPC UA packets per second in the manufacturing cell.

Figure 11 depicts the packet exchange between each production module and MES. The total amount of network traffic requires less than 1% of the total network transmission capability and even if it presents different types of traffic, there are no limitations that require service quality configurations (QoS). However, in a situation with a greater number of devices and equipment transmitting data in the network, a QoS configuration would become indispensable since the characteristics of the traffic are quite distinct.

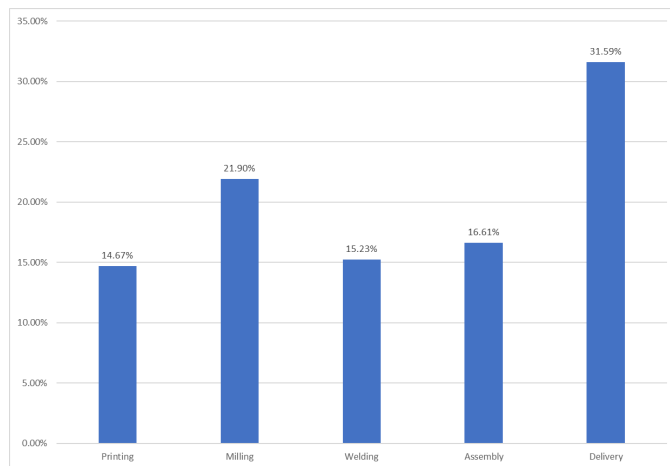


Figure 11. Data exchange between production modules and MES.

Although the OPC UA has very elastic response time requirements (response times from 1 to 10 s), it is interesting to separate the traffic into different queues to prevent bursts of other types of traffic affecting the OPC UA traffic.

The characteristic of this advanced manufacturing cell is that all modules perform their activities and report to the MES. There is no autonomy for a module to indicate its status to the next module. The integration between the protocols run by IPC was seen to be effective due to the absence of error messages or data retransmissions in addition to all the processes working in a synchronized way and performing the planned tasks.

6 Key challenges for advanced manufacturing cell

One of the key challenges to make legacy systems work with OPC UA is the development of a finite-state machine for each production module in order to determine how each piece of an OPC UA message and its parameters should be translated to the native industrial protocol of the production module.

Security issues are another key challenge of an advanced manufacturing cell since IPCs operate with regular operating systems quite similar to general-purpose computer operating systems. This means that such IPCs are suitable for security threats that usually do not exist in manufacturing cells with machines with limited or dedicated computational systems. To deal with such a challenge it is also necessary to use security technologies to guarantee data protection and integrity and also mechanisms to control access to the equipment. An advanced manufacturing cell may also be connected to the corporate network and even to the Internet as a way to be integrated with ERP, other managerial software, and also business partners.

A next-generation firewall was installed in the proposed manufacturing cell and data related to the module's performance were sent to a service in the cloud infrastructure on the Internet. The next-generation firewall installed was used only as a stateful firewall and controlled all communications to the external cloud, but OPC UA data or the communication between production modules and the servers (MES, ERP, PLM) was not analyzed. The firewall protected such servers from external attack. The firewall configuration includes in its rules the type of service, protocol, TCP and UDP port, IP source and destination, and the connection timeout (in order to avoid denial of service attacks).

The manufacturing cells constantly received access attempts from the Internet, and most of them must have been made by bots, since it was possible to observe a pattern in the traffic to discover open ports and services available, internal IP addresses, and other data about the infrastructure. During the evaluation of the cell, the WannaCry Trojan attack (The Economist, 2017) happened in the world and reached the manufacturing cell during the last two days of operation. The IPCs were running an operating system that could be affected by the attack. The developed firewall rules avoided the attack from the Internet, but this was insufficient since it would not protect direct access to the IPC from a person using a pen drive or any other type of storage system that could be infected by the offender code. To avoid an infection, some extra security mechanism should be implemented such as USB access blockage or deactivation of all services in the IPC not essential for its operation in the module. As antivirus software was not able to protect the machine against a new threat, it is also essential to have security policies to work with these technologies in a manufacturing cell.

7 Conclusions

The development of the proposed and described communication infrastructure used to evaluate the behavior of the OPC UA and its characteristics. The experiments detected several functionalities of OPC UA and some key messages about how to control the communication flow between two devices were explored. A strategy to integrate machines that do not work with OPC UA using an IPC as a gateway was also depicted and the effectiveness of such an approach was verified. The key point of this integration is the finite-state machine used to correctly map OPC UA message fields into other industrial protocols. Compared to other protocols running in the same infrastructure, the OPC UA demanded few resources from the communication infrastructure compared to its transmission capacity, since 1 Gbps is standard in an Ethernet network. The OPC UA framework promotes a low traffic overhead as well as it can be used to carry data from the traditional protocols in their fields without restrictions that could hinder the production. However, it is fragmented traffic since all packets are small compared to a maximum Ethernet frame size, which may produce effects related to traffic overhead such as jitter and delays. In such cases, the quality of service strategies would be an alternative to avoid failures of OPC UA. Security strategies are fundamental for an advanced manufacturing cell in any stage of development, since the IPCs works with general-purpose operating systems and because the production network would be interconnected with a corporative network or with the Internet as depicted in the proposed manufacturing cell. Future works include the evaluation of the OPC UA as a tool of integration between the IoT structures composed of sensors and actuators and the production environment and the evaluation of OPC UA security aspects.

References

- Acatech. (2013). *Recommendations for implementing the strategic initiative Industrie 4.0* (pp. 1-78). München: German National Academy of Science and Engineering.
- Drath, R., & Horch, A. (2014). Industrie 4.0: hit or hype? *IEEE Industrial Electronics Magazine*, 8(2), 56-58. <http://dx.doi.org/10.1109/MIE.2014.2312079>.
- Garcia, M. V., Irisarri, E., Perez, F., Estevez, E., & Marcos, M. (2016). OPC UA communications integration using a CPPS architecture. In *Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-6). New York: IEEE. <http://dx.doi.org/10.1109/ETCM.2016.7750838>.
- Godoy, A., & Perez, I. (2016). Integration of sensor and actuator networks and the SCADA system to promote the migration of the legacy flexible manufacturing system towards the Industry 4.0 concept. *Journal of Sensor and Actuator Networks*, 23(7), 1-21.
- Hoffmann, M., Thomas, P., Schutz, D., Vogel-Heuser, B., Meisen, T., & Jeschke, S. (2016). Semantic integration of multiagent systems using an OPC UA information modeling approach. In *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)* (pp. 744-747). New York: IEEE. <http://dx.doi.org/10.1109/INDIN.2016.7819258>.
- Industrial Internet Consortium – IIC. (2015). *Industrial Internet reference architecture* (pp. 1-101). Massachusetts.
- Jazdi, N. (2014). Cyber physical systems in the context of Industry 4.0. In *2014 IEEE International Conference on Automation, Quality and Testing, Robotics* (pp. 1-4). New York: IEEE. <http://dx.doi.org/10.1109/AQTR.2014.6857843>.
- Jiang, J. R. (2017). An improved cyber-physical systems architecture for Industry 4.0 smart factories. In *2017 International Conference on Applied System Innovation (ICASI)* (pp. 918-920). <http://dx.doi.org/10.1109/ICASI.2017.7988589>.

- Jirkovsky, V., Obitko, M., Kadera, P., & Marik, V. (2018). Toward plug play cyber-physical system components. *IEEE Transactions on Industrial Informatics*, 14(6), 2803-2811. <http://dx.doi.org/10.1109/TII.2018.2794982>.
- Kalor, A. E., Guillaume, R., Nielsen, J. J., Mueller, A., & Popovski, P. (2018). Network slicing in Industry 4.0 applications: abstraction methods and end-to-end analysis. *IEEE Transactions on Industrial Informatics*, 14(12), 5419-5427. <http://dx.doi.org/10.1109/TII.2018.2839721>.
- Kang, H., Lee, J., Choi, S., Kim, H., Park, J., Son, J., Kim, B. H., & Noh, S. (2016). Smart manufacturing: past research, present findings, and future directions. *International Journal of Precision Engineering and Manufacturing Green Technology*, 3(1), 111-128. <http://dx.doi.org/10.1007/s40684-016-0015-5>.
- Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, 6, 1-10. <http://dx.doi.org/10.1016/j.jii.2017.04.005>.
- Mahnke, W., Leitner, S.-H., & Damm, M. (2009). *OPC unified architecture*. Berlin: Springer. <http://dx.doi.org/10.1007/978-3-540-68899-0>.
- Müller, M., Wings, E., & Bergmann, L. (2017, July). Developing open source cyber-physical systems for service-oriented architectures using OPC UA. In *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)* (pp. 83-88). New York: IEEE. <http://dx.doi.org/10.1109/INDIN.2017.8104751>.
- OPC Foundation. (2017). *OPC unified architecture part 1: overview and concepts. OPC 10000-1. Release 1.04*. Scottsdale, AZ.
- Pedone, G., & Mezgar, L. (2018). Model similarity evidence and interoperability affinity in cloud-ready Industry 4.0 technologies. *Computers in Industry*, 100, 278-286. <http://dx.doi.org/10.1016/j.compind.2018.05.003>.
- Perez, F., Irisarri, E., Orive, D., Marcos, M., & Estevez, E. (2015). A CPPS architecture approach for Industry 4.0. In *2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)* (pp. 1-4). New York: IEEE.
- Profanter, S., Tekat, A., Dorofeev, K., Rickert, M., & Knoll, A. (2019). OPC UA versus ROS, DDS, and MQTT: performance evaluation of Industry 4.0 protocols. In *Proceedings of the IEEE International Conference on Industrial Technology (ICIT)*. New York: IEEE. <http://dx.doi.org/10.1109/ICIT.2019.8755050>.
- Schlechtendahl, J., Keinert, M., Kretschmer, F., Lechler, A., & Verl, A. (2015). Making existing production systems Industry 4.0-ready. *Production Engineering*, 9(1), 143-148. <http://dx.doi.org/10.1007/s11740-014-0586-3>.
- Schwab, K. (2016). *The fourth industrial revolution*. The World Economic Forum.
- Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, 14(11), 4724-4734. <http://dx.doi.org/10.1109/TII.2018.2852491>.
- Tang, D., Zheng, K., Zhang, H., Zhang, Z., Sang, Z., Zhang, T., Espinosa-Oviedo, J.-A., & Vargas-Solar, G. (2018). Using autonomous intelligence to build a smart shop floor. *International Journal of Advanced Manufacturing Technology*, 94(5-8), 1597-1606. <http://dx.doi.org/10.1007/s00170-017-0459-y>.
- Terzimehic, T., Wenger, M., Zoitl, A., Bayha, A., Becker, K., Muller, T., & Schauerer, H. (2017). Towards an Industry 4.0 compliant control software architecture using IEC 61499 OPC UA. In *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1-4). New York: IEEE.
- The Economist. (2017, May 20). *The WannaCry attack reveals the risks of a computerised world*. Retrieved in 2018, July 30, from <https://www.economist.com/leaders/2017/05/20/the-wannacry-attack-reveals-the-risks-of-a-computerised-world>

- Trotta, D., & Garengo, P. (2018). Industry 4.0 key research topics: a bibliometric review. In *2018 7th International Conference on Industrial Technology and Management (ICITM)* (pp. 113-117). New York: IEEE. <http://dx.doi.org/10.1109/ICITM.2018.8333930>.
- VDI/VDE-GMA Society for Measurement and Automatic Control. (2015). *Reference Architecture Model Industrie 4.0 (RAMI4.0)* (pp. 1-25). Düsseldorf: VDI – Verein Deutscher Ingenieure e.V., ZVEI – German Electrical and Electronic.
- Veichtlbauer, A., Ortmyer, M., & Heistracher, T. (2017, July). OPC UA integration for field devices. In *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)* (pp. 419-424). New York: IEEE. <http://dx.doi.org/10.1109/INDIN.2017.8104808>.
- Vogel-Heuser, B., Wildermann, S., & Teich, J. (2017). Towards the co-evolution of industrial products and its production systems by combining models from development and hardware/software deployment in cyber-physical systems. *Production Engineering*, 11(6), 687-694. <http://dx.doi.org/10.1007/s11740-017-0765-0>.
- Wan, J., Chen, B., Imran, M., Tao, F., Li, D., Liu, C., & Ahmad, S. (2018). Toward dynamic resources management for IoT-based manufacturing. *IEEE Communications Magazine*, 56(2), 52-59. <http://dx.doi.org/10.1109/MCOM.2018.1700629>.
- Wang, S., Ouyang, J., Li, D., & Liu, C. (2017). An integrated industrial ethernet solution for the implementation of smart factory. *IEEE Access : Practical Innovations, Open Solutions*, 5, 25455-25462. <http://dx.doi.org/10.1109/ACCESS.2017.2770180>.
- Zarte, M., Pechmann, A., Wermann, J., Gosewehr, F., & Colombo, A. W. (2016). Building an Industry 4.0-compliant lab environment to demonstrate connectivity between shop floor and IT levels of an enterprise. In *IECON 2016 – 42nd Annual Conference of the IEEE Industrial Electronics Society* (pp. 6590-6595). New York: IEEE.
- Zezulka, F., Marcon, P., Bradac, Z., Arm, J., Benesl, T., & Vesely, I. (2018). Communication systems for Industry 4.0 and the IIoT. *IFAC-PapersOnLine*, 51(6), 150-155. <http://dx.doi.org/10.1016/j.ifacol.2018.07.145>.