UNED

EIDUNED
Escuela
Internacional
de Doctorado

ACREDITACIÓN PUBLICACIONES PREVIAS

TESIS DOCTORAL:

MQTT-SCACAUTH: Esquema de seguridad para el protocolo MQTT y su uso en el entorno del IIoT

EDUARDO BUETAS SANJUAN

Resumen de publicaciones:

TABLA RESUMEN				
	AÑO	**TÍTULO DE LA PUBLICACIÓN**	**REVISTA**	**J.C.R**
PUBLICACIÓN 1	2020	Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach	IEEE Access	3,745
PUBLICACIÓN 2	2020	A propagation breakdown management model for the industrial internet of things	COMPUTERS IN INDUSTRY	3,954

Publicación 1:

Título: Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach.

Autores: Eduardo Buetas Sanjuan, Ismael Abad, Jose A. Cerrada, Carlos Cerrada.

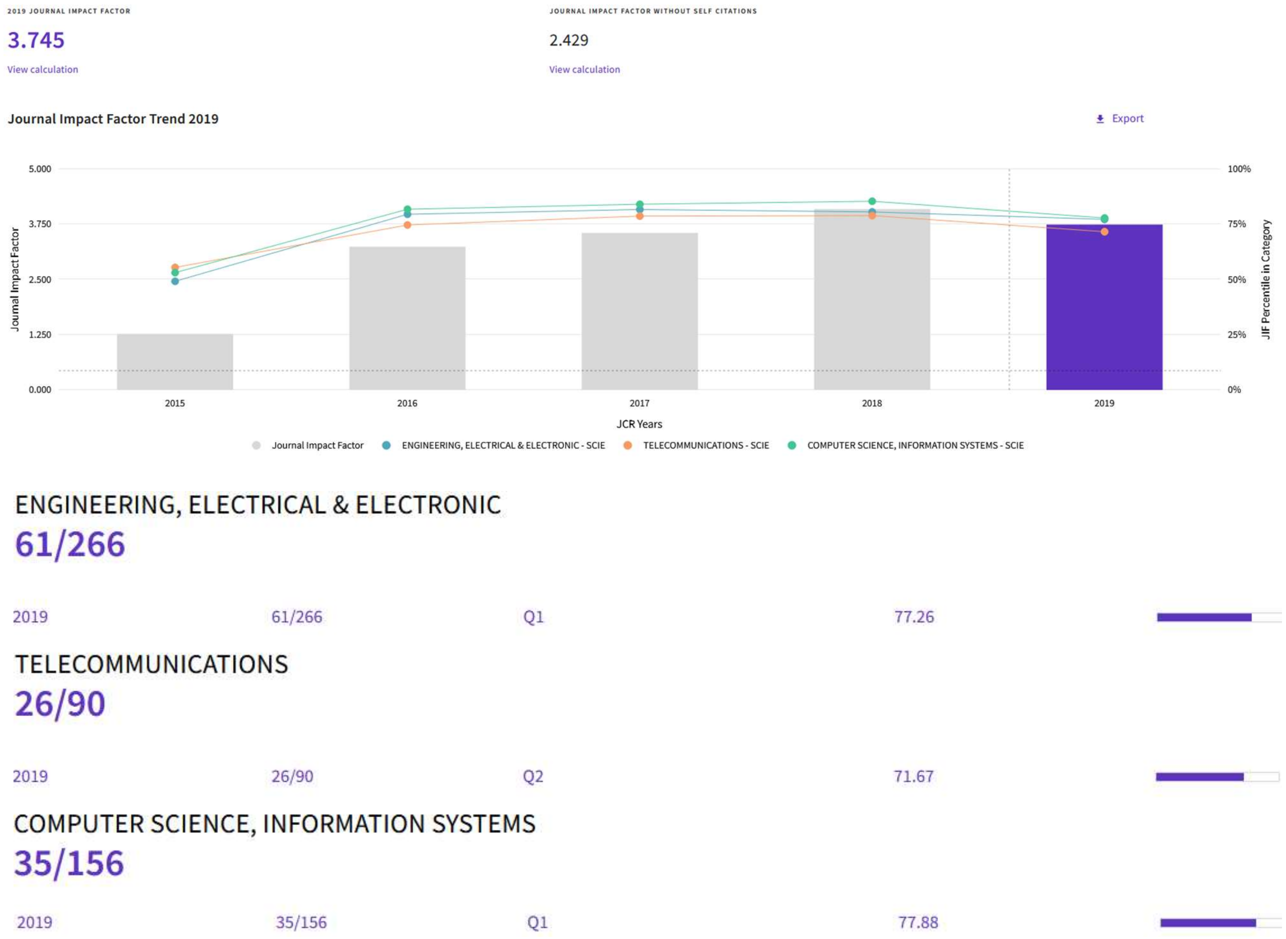
Revista: IEEE Access.

Año publicación: 2020.

Volumen: 8.

DOI: 10.1109/ACCESS.2020.3003998.

INDICE DE IMPACTO REVISTA :



2019 JOURNAL IMPACT FACTOR

3.745

View calculation

JOURNAL IMPACT FACTOR WITHOUT SELF CITATIONS

2.429

View calculation

Journal Impact Factor Trend 2019

Export
5.000
3.750
2.500
1.250
0.000
Journal Impact Factor
100%
75%
50%
25%
0%
JIF Percentile in Category
2015
2016
2017
2018
2019
JCR Years
Journal Impact Factor
ENGINEERING, ELECTRICAL & ELECTRONIC - SCIE
TELECOMMUNICATIONS - SCIE
COMPUTER SCIENCE, INFORMATION SYSTEMS - SCIE

ENGINEERING, ELECTRICAL & ELECTRONIC

61/266

2019	61/266	Q1	77.26

TELECOMMUNICATIONS

26/90

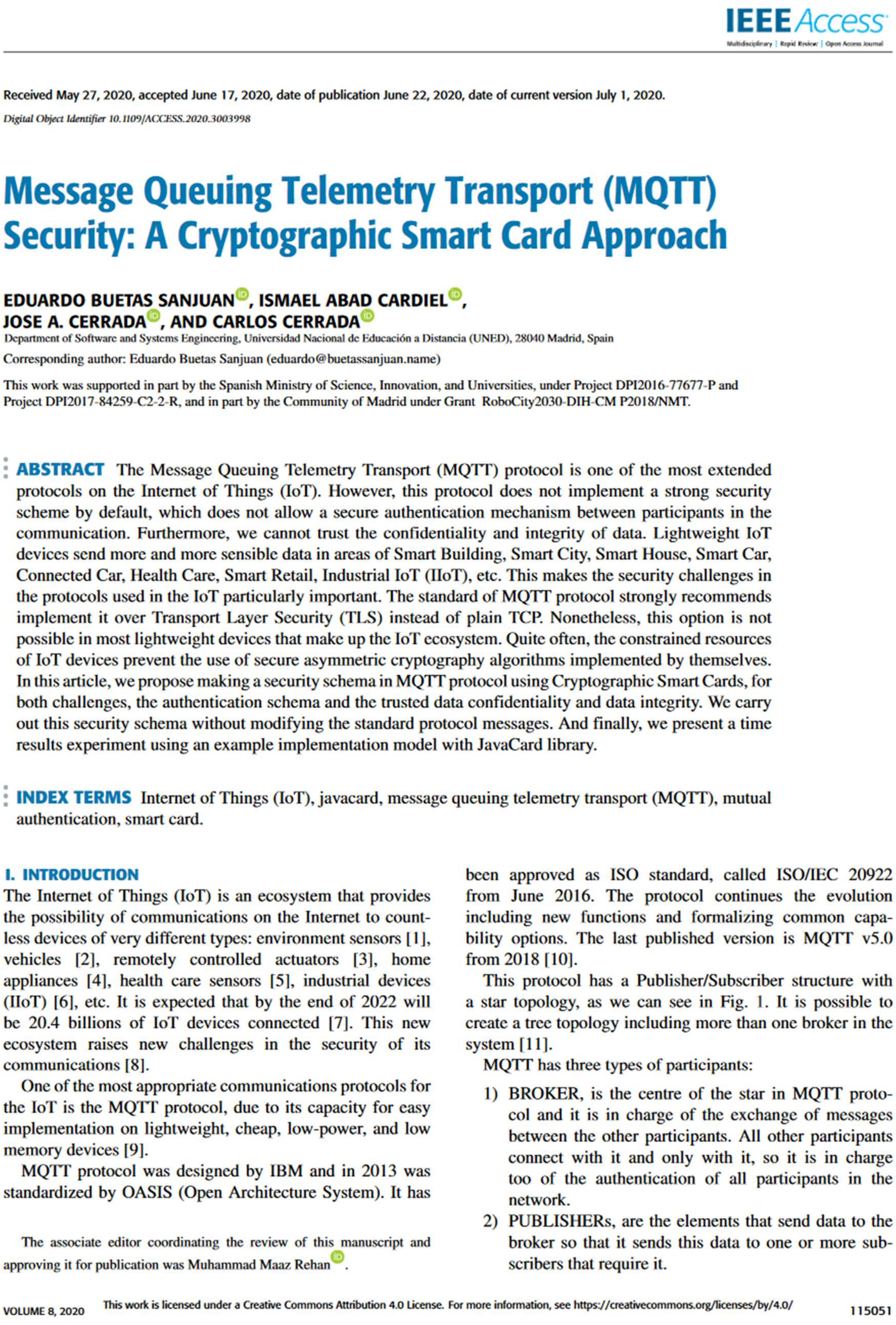
2019	26/90	Q2	71.67

COMPUTER SCIENCE, INFORMATION SYSTEMS

35/156

2019	35/156	Q1	77.88

PRIMERA PÁGINA PUBLICACIÓN:



IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 27, 2020, accepted June 17, 2020, date of publication June 22, 2020, date of current version July 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3003998

Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach

EDUARDO BUETAS SANJUAN, ISMAEL ABAD CARDIEL, JOSE A. CERRADA, AND CARLOS CERRADA
Department of Software and Systems Engineering, Universidad Nacional de Educación a Distancia (UNED), 28040 Madrid, Spain

Corresponding author: Eduardo Buetas Sanjuan (eduardo@buetassanjuan.name)

This work was supported in part by the Spanish Ministry of Science, Innovation, and Universities, under Project DPI2016-77677-P and Project DPI2017-84259-C2-2-R, and in part by the Community of Madrid under Grant RoboCity2030-DIH-CM P2018/NMT.

ABSTRACT The Message Queuing Telemetry Transport (MQTT) protocol is one of the most extended protocols on the Internet of Things (IoT). However, this protocol does not implement a strong security scheme by default, which does not allow a secure authentication mechanism between participants in the communication. Furthermore, we cannot trust the confidentiality and integrity of data. Lightweight IoT devices send more and more sensible data in areas of Smart Building, Smart City, Smart House, Smart Car, Connected Car, Health Care, Smart Retail, Industrial IoT (IIoT), etc. This makes the security challenges in the protocols used in the IoT particularly important. The standard of MQTT protocol strongly recommends implement it over Transport Layer Security (TLS) instead of plain TCP. Nonetheless, this option is not possible in most lightweight devices that make up the IoT ecosystem. Quite often, the constrained resources of IoT devices prevent the use of secure asymmetric cryptography algorithms implemented by themselves. In this article, we propose making a security schema in MQTT protocol using Cryptographic Smart Cards, for both challenges, the authentication schema and the trusted data confidentiality and data integrity. We carry out this security schema without modifying the standard protocol messages. And finally, we present a time results experiment using an example implementation model with JavaCard library.

INDEX TERMS Internet of Things (IoT), javacard, message queuing telemetry transport (MQTT), mutual authentication, smart card.

I. INTRODUCTION

The Internet of Things (IoT) is an ecosystem that provides the possibility of communications on the Internet to countless devices of very different types: environment sensors [1], vehicles [2], remotely controlled actuators [3], home appliances [4], health care sensors [5], industrial devices (IIoT) [6], etc. It is expected that by the end of 2022 will be 20.4 billions of IoT devices connected [7]. This new ecosystem raises new challenges in the security of its communications [8].

One of the most appropriate communications protocols for the IoT is the MQTT protocol, due to its capacity for easy implementation on lightweight, cheap, low-power, and low memory devices [9].

MQTT protocol was designed by IBM and in 2013 was standardized by OASIS (Open Architecture System). It has been approved as ISO standard, called ISO/IEC 20922 from June 2016. The protocol continues the evolution including new functions and formalizing common capability options. The last published version is MQTT v5.0 from 2018 [10].

This protocol has a Publisher/Subscriber structure with a star topology, as we can see in Fig. 1. It is possible to create a tree topology including more than one broker in the system [11].

MQTT has three types of participants:

1) BROKER, is the centre of the star in MQTT protocol and it is in charge of the exchange of messages between the other participants. All other participants connect with it and only with it, so it is in charge too of the authentication of all participants in the network.
2) PUBLISHERs, are the elements that send data to the broker so that it sends this data to one or more subscribers that require it.

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Maaz Rehan.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

Publicación 2:

Título: A propagation breakdown management model for the industrial internet of things

Autores: Eduardo Buetas Sanjuan, Ismael Abad, Jose A. Cerrada, Carlos Cerrada.

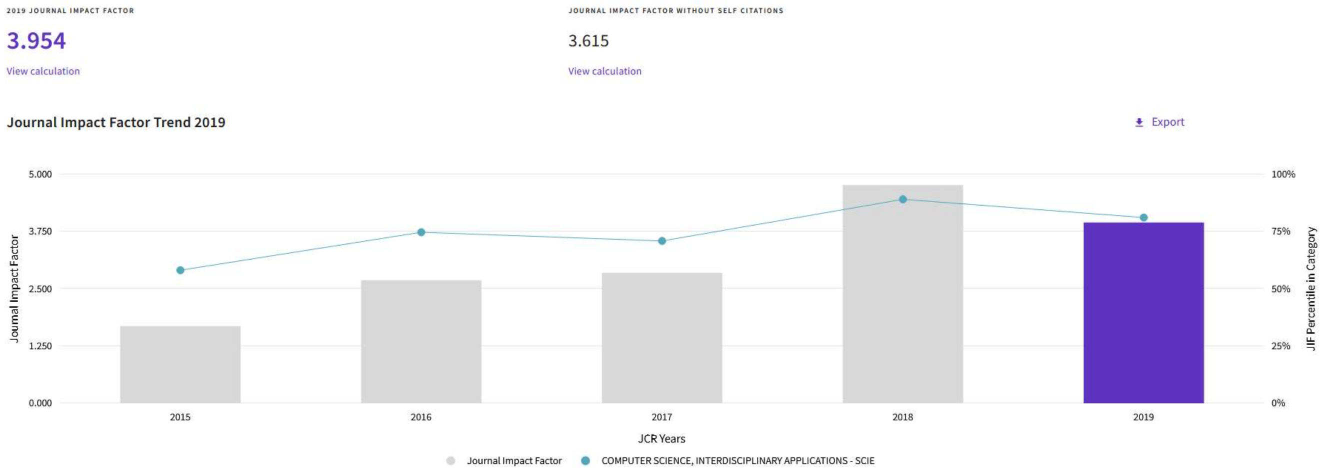
Revista: Computers in Industry.

Año publicación: 2020.

Volumen: 123.

DOI: 10.1016/j.compind.2020.103305 .

INDICE DE IMPACTO REVISTA :



2019 JOURNAL IMPACT FACTOR

3.954

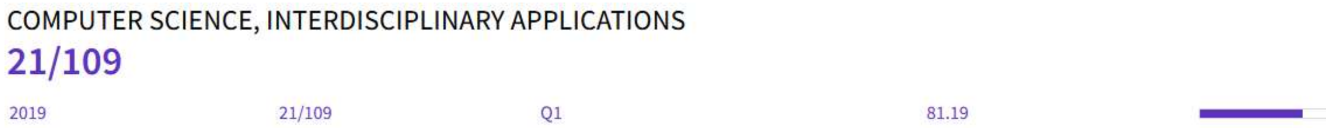
View calculation

JOURNAL IMPACT FACTOR WITHOUT SELF CITATIONS

3.615

View calculation

Journal Impact Factor Trend 2019

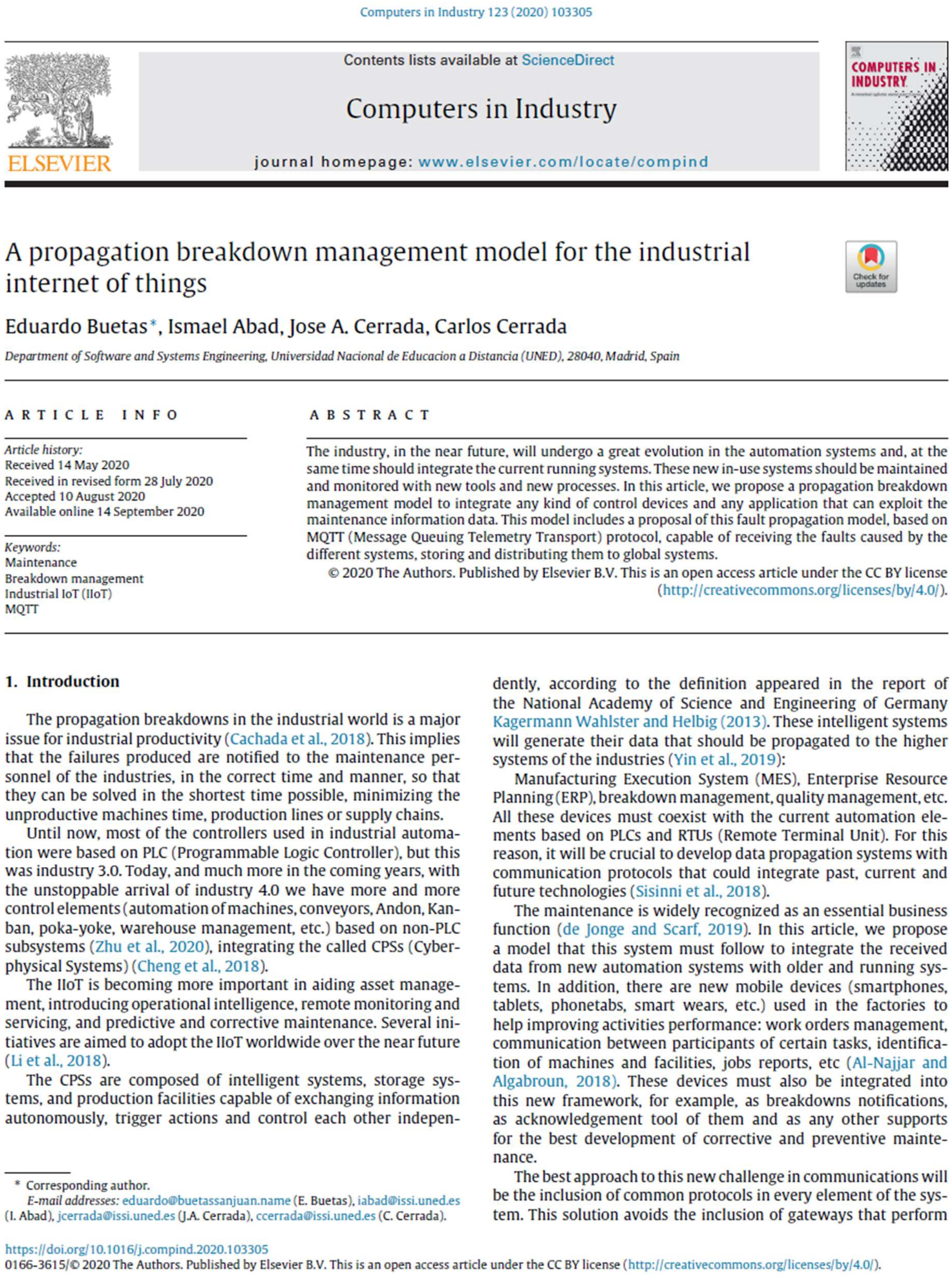


COMPUTER SCIENCE, INTERDISCIPLINARY APPLICATIONS

21/109

2019	21/109	Q1	81.19

PRIMERA PÁGINA PUBLICACIÓN:



Computers in Industry 123 (2020) 103305

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

A propagation breakdown management model for the industrial internet of things

Eduardo Buetas*, Ismael Abad, Jose A. Cerrada, Carlos Cerrada

Department of Software and Systems Engineering, Universidad Nacional de Educacion a Distancia (UNED), 28040, Madrid, Spain

ARTICLE INFO

Article history:
Received 14 May 2020
Received in revised form 28 July 2020
Accepted 10 August 2020
Available online 14 September 2020

Keywords:
Maintenance
Breakdown management
Industrial IoT (IIoT)
MQTT

ABSTRACT

The industry, in the near future, will undergo a great evolution in the automation systems and, at the same time should integrate the current running systems. These new in-use systems should be maintained and monitored with new tools and new processes. In this article, we propose a propagation breakdown management model to integrate any kind of control devices and any application that can exploit the maintenance information data. This model includes a proposal of this fault propagation model, based on MQTT (Message Queuing Telemetry Transport) protocol, capable of receiving the faults caused by the different systems, storing and distributing them to global systems.

© 2020 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

The propagation breakdowns in the industrial world is a major issue for industrial productivity (Cachada et al., 2018). This implies that the failures produced are notified to the maintenance personnel of the industries, in the correct time and manner, so that they can be solved in the shortest time possible, minimizing the unproductive machines time, production lines or supply chains.

Until now, most of the controllers used in industrial automation were based on PLC (Programmable Logic Controller), but this was industry 3.0. Today, and much more in the coming years, with the unstoppable arrival of industry 4.0 we have more and more control elements (automation of machines, conveyors, Andon, Kanban, poka-yoke, warehouse management, etc.) based on non-PLC subsystems (Zhu et al., 2020), integrating the called CPSs (Cyber-physical Systems) (Cheng et al., 2018).

The IIoT is becoming more important in aiding asset management, introducing operational intelligence, remote monitoring and servicing, and predictive and corrective maintenance. Several initiatives are aimed to adopt the IIoT worldwide over the near future (Li et al., 2018).

The CPSs are composed of intelligent systems, storage systems, and production facilities capable of exchanging information autonomously, trigger actions and control each other independently, according to the definition appeared in the report of the National Academy of Science and Engineering of Germany Kagermann Wahlster and Helbig (2013). These intelligent systems will generate their data that should be propagated to the higher systems of the industries (Yin et al., 2019):

Manufacturing Execution System (MES), Enterprise Resource Planning (ERP), breakdown management, quality management, etc. All these devices must coexist with the current automation elements based on PLCs and RTUs (Remote Terminal Unit). For this reason, it will be crucial to develop data propagation systems with communication protocols that could integrate past, current and future technologies (Sisinni et al., 2018).

The maintenance is widely recognized as an essential business function (de Jonge and Scarf, 2019). In this article, we propose a model that this system must follow to integrate the received data from new automation systems with older and running systems. In addition, there are new mobile devices (smartphones, tablets, phonetabs, smart wears, etc.) used in the factories to help improving activities performance: work orders management, communication between participants of certain tasks, identification of machines and facilities, jobs reports, etc (Al-Najjar and Algabroun, 2018). These devices must also be integrated into this new framework, for example, as breakdowns notifications, as acknowledgement tool of them and as any other supports for the best development of corrective and preventive maintenance.

The best approach to this new challenge in communications will be the inclusion of common protocols in every element of the system. This solution avoids the inclusion of gateways that perform

* Corresponding author.
E-mail addresses: eduardo@buetassanjuan.name (E. Buetas), iabad@issi.uned.es (I. Abad), jcerrada@issi.uned.es (J.A. Cerrada), ccerrada@issi.uned.es (C. Cerrada).

https://doi.org/10.1016/j.compind.2020.103305
0166-3615/© 2020 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).