




Editorial

Emerging Paradigms and Architectures for Industry 4.0 Applications

Paula Fraga-Lamas ^{1,2,*} , Sérgio Ivan Lopes ^{3,4,5}  and Tiago M. Fernández-Caramés ^{1,2} 

¹ Department of Computer Engineering, Faculty of Computer Science, Universidade da Coruña, 15071 A Coruña, Spain

² Centro de Investigación CITIC, Universidade da Coruña, 15071 A Coruña, Spain

³ ADiT-Lab, Instituto Politécnico de Viana do Castelo, 4900-348 Viana do Castelo, Portugal

⁴ CiTin—Centro de Interface Tecnológico Industrial, 4970-786 Arcos de Valdevez, Portugal

⁵ IT—Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

* Correspondence: paula.fraga@udc.es; Tel.: +34-981-167-000

1. Introduction

The Fourth Industrial Revolution (4IR), called “Industry 4.0” in Europe, “Industrial Internet of Things” in North America, or “Made in China 2025” in China, blurs the boundaries between the physical, digital and biological worlds, paving the way to the continuous improvement of manufacturing processes. The 4IR-enabling technologies such as Industrial Cyber-Physical Systems (ICPS), Industrial Internet of Things (IIoT) technologies, novel computing paradigms (e.g., fog, mist, and edge computing), Distributed Ledger Technologies (DLTs) (e.g., blockchain), digital twins, and augmented/mixed reality technologies, enable novel cyber-secure, resilient, collaborative and human-centric advanced manufacturing systems. Such systems focus on the continuous improvement of the manufacturing processes, by taking advantage of several relevant digitalization-related aspects: (1) at the data level, i.e., collection, communication, and storage; (2) at the system’s operational level, i.e., reliability, scalability, real-time, and energy efficiency; and (3) at the systems’ integration level, i.e., interoperability, standardization, and security by design.

This Special Issue aims to report the latest breakthroughs in architectures, paradigms, and applications in the ever-increasing complex ecosystem of smart manufacturing. A total of eleven research papers were published in this Special Issue, approaching several fields of Industry 4.0 paradigm, such as Low-Power Wide-Area Network (LPWAN) technologies, additive manufacturing, energy harvesting, Industrial Internet of Things (IIoT), Cyber-Physical Systems (CPS), Artificial Intelligence (AI) or cybersecurity.

Specifically, in [1], the authors analyzed the challenges related to the deployment of future industrial networks for process automation. To illustrate such an analysis, traffic measurements have been performed with a pulp and paper mill, which allow them to determine representative traffic characteristics for process automation.

Many future industrial networks will have to deal with enormous amounts of data that will be later processed and analyzed through Big Data techniques, which will require massively parallel computers (MPCs), whose interconnection through conventional topologies is unfeasible. For such a reason, in [2], Rahman et al. have studied the hierarchical interconnection networks (HINs), proposing a novel HIN that is a Tori-connected Flattened Butterfly Network (TFBN). Such a network architecture is first described and then its performance is analyzed in terms of static network performance and cost-effectiveness.

Low-power networks have been studied in [3,4]. In [4], the authors present the development of an optimized Adaptive Data Rate (ADR) mechanism for the LoRaWAN uplink and downlink, which has been evaluated in an industrial scenario in terms of packet loss and energy. Regarding [3], the authors first focused on reviewing the security vulnerabilities that exist in LPWANs, and then present an attack vector analysis specifically



Citation: Fraga-Lamas, P.; Lopes, S.I.; Fernández-Caramés, T.M. Emerging Paradigms and Architectures for Industry 4.0 Applications. *Appl. Sci.* **2022**, *12*, 9546. <https://doi.org/10.3390/app12199546>

Received: 20 September 2022

Accepted: 21 September 2022

Published: 23 September 2022

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

designed for the IoT ecosystem. Thus, the paper identifies security vulnerabilities that impact LPWAN communications technologies and suggests mitigation measures to tackle with the identified vulnerabilities.

Cybersecurity for industrial systems is the common theme in [5–7]. With respect to [5], the authors focus on the development of time-predictable and secure embedded systems, and then extend the discussion to time-critical and secure CPSs. Moreover, the presented work identifies the gaps in the existing frameworks and techniques for the development of time- and safety-critical CPSs and analyzes the opportunities that artificial intelligence can provide in the development of such systems. Regarding the work described in [6], it is proposed a certificate-based authentication system that uses a secondary device in IIoT scenarios. In the proposed system, the user's sign key is encrypted with a secret key that can be computed with his/her password, while a secret parameter is stored in a secondary device to protect the key. The feasibility of such a system is shown through a prototype that made use of standard cryptographic algorithms (AES-256, RSA-3072, and ECDSA-256), whose performance and security are evaluated. In [7], the authors propose a novel methodology to learn Industry 4.0 and IIoT cybersecurity through practical use cases carried out with the help of free online tools such as Shodan. The described approach was tested during the COVID-19 pandemic lockdowns, showing that students were able to find that 13% of the analyzed IIoT/Industry 4.0 systems could be accessed really easily. Thus, the article provides useful guidelines for teaching industrial cybersecurity and thus trains the next generation of security researchers and developers.

Other relevant Industry 4.0 technologies were studied in [8–10]. In [8], the authors analyze the problem of how to monitor and control additive manufacturing processes in real-time. With such a purpose, the paper identifies real-time machine learning algorithms to analyze the received data and then execute control functions, and then proposes a new architecture, which is illustrated through a practical industrial example. Regarding the work detailed in [9], it analyzes in detail the operation principles of a wind harvester to obtain its characteristic parameters and to create an equivalent electromechanical model. The accuracy of such a model is verified through a prototype, whose AC/DC converter architecture was optimized in terms of parameters such as efficiency, voltage levels, operation frequency, duty cycle, or load. With respect to [10], a perceptual system is proposed to simulate the ventral flow of the human perception system. The main objective of the proposed solution is to simulate human senses that can be later used to estimate user comfort. For such a purpose, a Spatio-temporal Convolutional Neural Network (S-CNN) and a concatenated HoppingNet temporal CNN (T-CNN) are used. The shown results indicate that the proposed system is highly accurate and robust.

Finally, in [11], the authors provide an integrated reference model for digital manufacturing platforms, which is based on cutting-edge reference models for IIoT. Thus, the article analyzes the most relevant reference models for IIoT systems to align their definitions and to determine to what extent they are complementary. As a result, the Industrial Internet Integrated Reference Model (I3RM) for digital manufacturing platforms is presented, together with general recommendations that can be applied to the architectural definition of any digital manufacturing platform.

Author Contributions: All authors contributed equally to the article. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been supported through funds ED431G 2019/01 provided by Centro de Investigación de Galicia "CITIC" for a research stay in Instituto Técnico de Viana do Castelo. This work has also been funded by the Xunta de Galicia (by grant ED431C 2020/15), the Agencia Estatal de Investigación of Spain (by grants PID2020-118857RA-I00 and PID2019-104958RB-C42) and ERDF funds of the EU (FEDER Galicia 2014–2020 & AEI/FEDER Programs, UE).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

4IR	Fourth Industrial Revolution
AI	Artificial Intelligence
CPS	Cyber–Physical System
IIoT	Industrial Internet of Things
ICPS	Industrial Cyber–Physical System
DLT	Distributed Ledger Technology
LPWAN	Low-Power Wide-Area Network
HIN	Hierarchical Interconnection Network
MPC	Massively Parallel Computer
TFBN	Tori-connected Flattened Butterfly Network
ADR	Adaptative Data Rate
S-CNN	Spatio-temporal Convolutional Neural Network
T-CNN	Concatenated HoppingNet temporal CNN

References

1. Åkerberg, J.; Furunäs Åkesson, J.; Gade, J.; Vahabi, M.; Björkman, M.; Lavassani, M.; Nandkumar Gore, R.; Lindh, T.; Jiang, X. Future Industrial Networks in Process Automation: Goals, Challenges, and Future Directions. *Appl. Sci.* **2021**, *11*, 3345. [[CrossRef](#)]
2. Rahman, M.M.H.; Al-Naem, M.; Ali, M.N.M.; Sufian, A. TFBN: A Cost Effective High Performance Hierarchical Interconnection Network. *Appl. Sci.* **2020**, *10*, 8252. [[CrossRef](#)]
3. Torres, N.; Pinto, P.; Lopes, S.I. Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem. *Appl. Sci.* **2021**, *11*, 3176. [[CrossRef](#)]
4. Todoli-Ferrandis, D.; Silvestre-Blanes, J.; Sempere-Payá, V.; Planes-Martínez, A. Analysis of Bidirectional ADR-Enabled Class B LoRaWAN Networks in Industrial Scenarios. *Appl. Sci.* **2020**, *10*, 7964. [[CrossRef](#)]
5. Mubeen, S.; Lisova, E.; Vulgarakis Feljan, A. Timing Predictability and Security in Safety-Critical Industrial Cyber–Physical Systems: A Position Paper. *Appl. Sci.* **2020**, *10*, 3125. [[CrossRef](#)]
6. Choi, J.; Cho, J.; Kim, H.; Hyun, S. Towards Secure and Usable Certificate-Based Authentication System Using a Secondary Device for an Industrial Internet of Things. *Appl. Sci.* **2020**, *10*, 1962. [[CrossRef](#)]
7. Fernández-Caramés, T.; Fraga-Lamas, P. Use Case Based Blended Teaching of IIoT Cybersecurity in the Industry 4.0 Era. *Appl. Sci.* **2020**, *10*, 5607. [[CrossRef](#)]
8. Adnan, M.; Lu, Y.; Jones, A.; Cheng, F.-T.; Yeung, H. A New Architectural Approach to Monitoring and Controlling AM Processes. *Appl. Sci.* **2020**, *10*, 6616. [[CrossRef](#)]
9. Pozo, B.; Araujo, J.Á.; Zessin, H.; Mateu, L.; Garate, J.I.; Spies, P. Mini Wind Harvester and a Low Power Three-Phase AC/DC Converter to Power IoT Devices: Analysis, Simulation, Test and Design. *Appl. Sci.* **2020**, *10*, 6347. [[CrossRef](#)]
10. Fang, X.; Fang, H.; Feng, Z.; Wang, J.; Zhou, L. Artificial Auditory Perception Pattern Recognition System Based on Spatiotemporal Convolutional Neural Network. *Appl. Sci.* **2020**, *10*, 139. [[CrossRef](#)]
11. Fraile, F.; Sanchis, R.; Poler, R.; Ortiz, A. Reference Models for Digital Manufacturing Platforms. *Appl. Sci.* **2019**, *9*, 4433. [[CrossRef](#)]