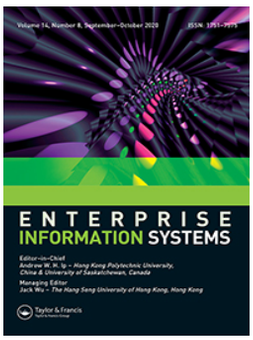

Enterprise Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/teis20

Interoperability enablers for cyber-physical enterprise systems

Ricardo Jardim-Goncalves, David Romero, Diogo Goncalves & João Pedro Mendonça

To cite this article: Ricardo Jardim-Goncalves, David Romero, Diogo Goncalves & João Pedro Mendonça (2020) Interoperability enablers for cyber-physical enterprise systems, Enterprise Information Systems, 14:8, 1061-1070, DOI: 10.1080/17517575.2020.1815084

To link to this article: https://doi.org/10.1080/17517575.2020.1815084

ENTERPRISE INFORMATION SYSTEMS
2020, VOL. 14, NO. 8, 1061–1070
https://doi.org/10.1080/17517575.2020.1815084

Taylor & Francis
Taylor & Francis Group

EDITORIAL

Interoperability enablers for cyber-physical enterprise systems

1. Introduction

According to telecom giant CISCO (2013), the *Internet of Everything (IoE)* is 'bringing together people, processes, data, and things to make networked connections more relevant and valuable than ever before, turning information into actions that create new capabilities, richer experiences, and unprecedented socio-economic and environmental opportunities for businesses and individuals'.

In this context, the *Future Internet-based Enterprise Information Systems* can be defined as 'an enterprise-centric network integrating and interoperating with proprietary and non-proprietary advanced technologies, computers, communication systems, control strategies as well as cognitive agents (both humans and/or advanced intelligent systems) able not only to manage people, processes and things but also to generate new behaviours for adapting themselves to a dynamic market' (adapted from Davis, Eisenhardt, and Bingham 2007) (Panetto et al. 2015). State-of-the-Art technology has empowered a systematical deployment of Cyber-Physical Systems (CPS) to the Enterprise Systems (Romero and Vernadat 2015), enabling information from heterogeneous physical and virtual sources to be closely monitored and synchronised between the *physical* and the *cyber-computational* spaces, providing mechanisms for advanced data analytics with networked capabilities able to perform collaboratively, resiliently and more efficiently towards the visionary *Enterprise of the Future (EoF)*.

This paper seeks to bring together, and to summarise as editorial, the novel contributions from researchers and practitioners that published in this special issue, who are exploring the definition and applicability of *'Cyber-Physical Enterprise Systems Interoperability'*, in a global perspective to contribute to reaching the visionary Enterprise of the Future; putting the focus on novel strategies, methods and tools in a scientific-based standpoint. Conceptual, theoretical, empirical and technological contributions are foreseen, illustrated by applied examples and convincingly demonstrating noteworthy novelty in comparison with previously reported results.

2. Enterprise interoperability and cyber-physical enterprise systems

As information systems in enterprises and organisations evolve and become more complex, the need for interoperable operation, automated data interchange and coordinated behaviour of large-scale infrastructures becomes highly critical (Jardim-Goncalves, Steiger-Garcao, and Agostinho 2010). Apart from being a technical issue, interoperability challenges also appear at an organisational and semantic level, underlying the need for patterns and solutions that support the seamless cooperation among ICT systems,

information and knowledge, organisational structures and people (Jardim-Goncalves, Grilo, and Steiger-Garcao 2006a).

The ability and capability of enterprises to collaborate has been closely linked to the ability and capability of enterprises to interoperate. A key premise is that *Enterprise Interoperability* is a key enabler for 'networked organizations'. The adoption of advanced techniques for meta-modelling and automatisms for model and data transformations will enable to have the engine for interoperability not embedded directly in the system's coding, but through proper adaptative techniques get a suitable characterisation of the actual status of the system's morphisms, supporting predictive system evolution, and analysis of its complexity in the dynamics of the network, including the respective transients and systems responsive behaviour.

Hence, *Enterprise Interoperability (EI)* is a well-established area of applied research that addresses the problems related to the lack of systems and applications' interoperability in organisations and proposes novel solutions for EI problems. However, despite research efforts to date, there is still a lack preventing the generalisation and full reuse of the methods and tools that have been developed so far and is threatening the sustainability of EI as a domain for research in the advent of *Cyber-Physical Enterprise Systems* concept. Enterprises are today confronted with increasingly global and dynamic markets and are consequently driven to reshape their strategies to meet the challenges of the 21st Century concerning competitiveness, productivity, and sustainability.

However, many companies and especially SMEs and Mid-Caps, are struggling to incorporate cyber-physical, embedded or IoT systems into their products, do not yet understand the lifecycle-wide potential of data and information sourced from them for adding value, do not have the multi-disciplinary expertise required to implement such systems, or have difficulties accepting communicating or sharing product-related data over the Internet of Things.

Concerning the situation today, primarily local initiatives on Industry 4.0 and advanced automation were founded until now. However, they have a limited impact on the particular end-user of the technological innovation that arises from the interdisciplinary requirements profile. For example, DIH4CPS European project approaches this issue and provides the means for sustainable partnerships throughout the network as well as a solid business perspective for end-users in the application experiments.

DIH4CPS specifically does everything necessary to guarantee a sustainable and over-arching nature of its Network. The DIH4CPS network will provide significant benefits for enrolled DIHs by shaping, improving and extending their business models and customising their offered service landscape by implementing an Ecosystem-Technology-Business service catalogue for the Embedded and Cyber-Physical Systems domain. This way, enrolled DIHs will be empowered to find and highlight their Unique Value Proposition for end-users.

3. Novel contributions on cyber-physical enterprise systems

3.1. Capability model for public administration interoperability

Cestari et al. (2019) in their paper *'A Capability Model for Public Administration Interoperability'* present a Public Administration Interoperability Capability Model

(PAICM) and describe its structure and the rationale adopted to compose its elements, explaining the selection and extraction of the attributes to their categorisation within the interoperability and public administration domain.

The paper addresses the research question 'how a capability model and a diagnosis method of interoperability, in the public administration domain, allows measuring an entity's level of potential interoperability?' proposing a framework methodology to diagnose the interoperability in a public administration scenario, including the capability model and the diagnosis method.

The definition of capability adopted in this research is based on Princeton University (2018), CMMI Product Team (2010) and ISO/IEC (2015), and can be described as (i) The measure of the ability of an entity to achieve its objectives; (ii) The ability to perform or achieve certain actions or outcomes through a set of controllable and measurable faculties (e.g., features, functions, processes, or services); and (iii) The degree of how good the implementation or achievement of some faculty is.

Using the research methodology typology proposed by Filippini (1997), it proposes a theoretical/conceptual capability model called the 'Public Administration Interoperability Capability Model (PAICM)', composed of attributes, guidelines and capability levels, describing the intervals of the capability degree of certain measurable attributes related to the interoperability domain.

Considering the originality aspects, the complexity presented in the public administration context requires additional effort regarding its influencing such as legal, political, socio-cultural and other issues. The PAICM structure and its components (viz. cards, attributes, description, and capability levels) are implemented for practical use to obtain two research outcomes: The first is the collection of spreadsheets that organise and materialise the model into usable artefacts, which can then be used to collect and store information during the diagnosis process according to the AHP method. The second outcome is the AHP model, which supports the structural representation requirements of the PAICM addressing the difficult process of diagnosing potential interoperability in the public administration domain.

3.2. Cloud-based platform for the non-invasive management of coronary artery disease

Currently, several platforms are available for public health and disease management. The paper '*A Cloud-based Platform for the Non-Invasive Management of Coronary Artery Disease*' by Sakellarios et al. (2020) proposes a cloud-based system using a mobile application that enables telemedicine services for the management of hypertensive patients (Zhou et al. 2019). Using this platform, patients' data are recorded automatically, reducing the healthcare costs while in parallel the doctor monitors the patient's status. Moreover, cloud-computing in combination with the Internet of Things is being used recently in prevention and predictive strategies taking the advantages of the cloud in terms of speed, security and integration.

This research was developed in the scope of the SMARTool project, developing a novel cloud-based platform for the management of CAD from the patient risk stratification using non-imaging data to CDSS for diagnosis, prognosis and disease treatment. The platform integrates several interoperability standards as well as cyber-physical systems,

including algorithms and software for the analysis of CTCA imaging and points of care devices (PoC) for capturing the monocytes and the I-CAM1 molecule in blood samples. The SMARTool platform is achieved by a unified and comprehensive solution, using information from cyber-physical systems integrated into a CDSS for risk stratification, diagnosis, prognosis and treatment. The design and the development of the platform were based on European and International standards to guarantee the privacy of any sensitive data handling, in particular the EU General Data Protection Regulation (GDPR). To acquire data from diverse data sources, the system provides a specific HL7 compliant integration layer using clinical data semantics.

3.3. Contextual self-organising of manufacturing process for mass-individualisation: a cyber-physical-social system approach

The Social Internet of Things (SIoT) concept (Atzoria et al. 2012) to handle the heterogeneity, as well as the boosting sociality among things, is tackled to develop a *'Contextual Self-Organizing of Manufacturing Process for Mass-Individualization: A Cyber-Physical-Social System Approach'* by Leng et al. (2018). In this work, to enable SIoT, a smart workpiece model is established and exposed to the Web allowing command and control-based interactions with prosumers and smart machines. Therefore, contextual-awareness is proposed to handle the variety of context data in a Cyber-Physical-Social System (CPSS) for proactive decision-making. The intelligence is generated from the perception of both objective context (i.e., the physical environment) and subjective context (i.e., the internal sociality aspects).

The recently proposed paradigmatic class of CPSS instantiates extracted knowledge hidden in activities, preferences, and various other subjective elements embedded from human behaviours. However, two challenges hindering the CPSS approach are identified, i.e., the heterogeneous complexity nature and the large-scale contextual data involved in CPSS.

Leng et al. (2018) propose key enabling techniques to achieve contextual self-organising of a manufacturing process for mass-individualisation. From the organisation perspective, a contextual-awareness strategy is a novel choice for the complex SIoT, in which a temporal social structure meets individuals' goals. Additionally, the proposed model also helps both workpieces and machines to finish the appropriate matchmaking since the SIoT informed them about their speciality, status and requirements.

Therefore, the SIoT results in a new decentralised intelligent way to realise mass individualisation in the manufacturing section, where SIoT monitors spatiotemporal situations in a spontaneous social network of relationships and interactions and induces relevant smart machines depending on prosumers' individual demands.

3.4. New formal paradigm to model redundancy and resiliency in cyber-physical systems

In *'Cyber-Physical Systems, A New Formal Paradigm to Model Redundancy and Resiliency'* by Lezoche and Panetto (2018), the authors adapted the Formal Concept Analysis (FCA) as a knowledge representation and discovery tool for the needs of CPS modelling and analysis. The proposed result highlights the FCA bottom-up approach focusing on the particularities of the domain and building upon them a structure to allow to discover the general

dependencies. Therefore, using a CPS meta-model formalisation and FCA, it proposes a way to optimise the modelling of CPS systems emphasising their redundancy and resiliency.

Two main results are identified from this research: (i) the presentation of a CPS meta-model that represents a first step towards the knowledge formalisation needed to structure the use of formal tools; and (ii) the FCA adaptation to this domain to find hidden knowledge thanks to the implicit relations existing in the structure of the system.

The use of the resulting lattice-models to response some of the pressing questions of Industry 4.0 such as the identification of redundancies in functionalities, the improvement of the systems plasticity and their auto-adaptation to environment changes, are identified as main challenges to address.

3.5. Bridging IoT devices with cloud infrastructures for interoperable telehealth platforms

Following the adaptation of Internet of Things (IoT) devices, telehealth applications have emerged into prominent solutions for improving patient management. Most platform designs, however, lacked the necessary interoperability to enable easy integration of different systems, devices or applications and allow un-intrusive data sharing between components and stakeholders. *'Designing Interoperable Telehealth Platforms: Bridging IoT Devices with Cloud Infrastructures'* by Tsiouris et al. (2020) proposes a platform offering Web technologies and interoperable components, to successfully integrate different technologies into a robust system. The platform is deployed by the HOLOBALANCE research project and validated in a telerehabilitation system for patients with balance disorders providing surrogate physiotherapist as a super-imposed hologram through augmented reality.

At the system level, interoperability in telehealth platforms facilitates the integration and communication of different modules and ensures that data are reusable and readily available to be shared without requiring additional effort by the end-user. An interoperable by-design platform is presented in this study, targeting telehealth rehabilitation applications. The proposed interoperable architecture streamlines communications and data exchange between independent modules, responsible for data storage, processing and advanced visualisation with virtual user interaction while facilitating the integration of 3rd party tools, off-the-shelf IoT devices and cloud infrastructures. The edge computing unit of the proposed platform handles the integration of different devices, which can be instantly connected, replaced or swapped, as long as they use standard communication protocols (e.g., Bluetooth, BLE, Wi-Fi, and USB).

Bottom line, the HOLOBALANCE platform contributes to the advancement of telehealth, which is a critical component of the evolving digital-health transformation, providing a more effective and efficient way to use limited staff and resources. Using holograms to deliver in-home coaching and precise sensor-based exercise monitoring, the proposed system empowers active engagement, improving access and quality of healthcare, and increasing convenience for both patients and domain experts.

3.6. Enterprise interoperability development in multi relation collaborations

Khisro and Sundberg (2018) present a study that aims to clarify what are the *success factors from the Danish electricity market* for overcoming issues of business process and data fragmentation in the development of *enterprise interoperability in multi relation collaborations*. A qualitative approach for an in-depth understanding of interviewees experiences of the subject and its conditions (Creswell 2014; Yin 2013). Documents, publications and the web about the energy market from the different parties in Denmark were used as background material in the empirical study for understanding the development situation (Yin 2013).

The analysis demonstrates that the data hub was a market project that influenced all enterprises involved and restructured the entire market. Creativity is needed to go beyond organisational boundaries and find new ways to communicate the change of both information systems and business activities to collaborate in a multi relation for clarifying what are the success factors for overcoming issues of business process and data fragmentation in the development of enterprise interoperability in multi relation collaborations. The identified success factors are those: related to general project management and change management; related to business processes; and related to information and data.

3.7. Literature review on autonomous production control methods

Martins et al. (2020) present a comprehensive 'Literature Review on Autonomous Production Control Methods', discussing the actual APC methods and highlighting future research directions.

Production control methods most in use today, are focused on centralised decision-making and planning and considered inadequate to deal with the increasing dynamics of these systems. To face this increasing complexity and dynamics, it is crucial to have effective production control methods, considering Interoperability Enablers for Cyber-Physical Systems.

Autonomous Production Control (APC) may be an adequate alternative to face this complexity, allowing a flexible and rapid reaction to possible disturbances that may occur in the production system. APC methods enable decentralised and autonomous control, which are key issues in Cyber-Physical Systems (CPS), and thus in the scope of Industry 4.0, were CPS is one of its main pillars. This requires high levels of interoperability capabilities among logistic objects, which is further based on enabling communication and processing technologies, such as RFID (radio frequency identification), along with other technologies, such as sensors and devices for data acquisition and data processing and analysis, playing a crucial role for supporting decision-making in APC methods. Nevertheless, Martins et al. (2020) suggest that APC methods are not being exploited to their full potential for decision-making in real-time, being exclusively used for job allocation purpose.

4. Interoperability considerations on technological and societal dimensions

The increased relevance of the Internet of Things (IoT) when applied to the enterprise dimension, stimulates the establishment of *Cyber-Physical Enterprise Systems* that

facilitated the emergence of new technologies in today's society. The ability to make value-added decisions comes at a price, more specifically the increased risk, which sensitive data may be exposed to when created and stored within networks. Therefore, risk management is a factor that must be highlighted when identifying the security implications of the emergence of IoT. From an economic perspective, the security implications present within the IoT does not deter the impact that it has on the productivity of a country's workforce, a key macroeconomic variable that is linked with a country's level of economic growth.

Therefore, the concept of risk management can be looked upon as critical when identifying approaches to ensure data security during the rise of IoT. The risk management strategies implemented by enterprises must be tailored depending on the potential risk presented. Firstly, the ability of IoT to increase the efficiency of manufacturing processes and supply chain networks relies heavily upon interoperability. The benefits yielded by interoperability in terms of increased labour productivity must be contrasted with the predominant threat of data exposure. This often occurs due to the absence of investment by enterprises to ensure that the IoT solutions implemented have been correctly tested for potential vulnerabilities (Toney 2016).

As technological advancements arise, businesses begin to cater for an increased utilisation of IoT solutions to improve and optimise operations whilst increasing labour productivity and output. As businesses accommodate the increased use of technology in their production processes, more weight is given to data security as it becomes an imperative focus of operational decision making and data-driven decisions. As this happens, risk management within businesses gains increased complexity. Businesses must, therefore, remain increasingly vigilant for possible risks attributed to the use of newly introduced technologies that despite having advantages, could also induce risks and vulnerabilities that could threaten user data security and privacy (Irfan Saif 2015).

IoT must be looked upon as a long-term investment for companies. A successful IoT solution must be one, which implements a structured approach by identifying threats and finding appropriate responses by reinforcing the principle of security. Given the high volume of sensitive data exchanged through IoT solutions that allow for value-added decisions to be made in real-time, data security must be looked upon as a critical factor for the success of IoT solutions within enterprises.

Ubiquitous developments of IoT technologies have the potential to impact the global economy and create real economic value. This said the increased use of intelligent systems and the pivotal focus on user data security and privacy could help IoT technologies reach its full potential resulting in vast economic impact and the development of real economic value for society as a whole.

To correctly identify areas within which IoT technologies are able to have the greatest value within the economy we must first look at the potential of IoT technologies in the global economy. For instance, Manyika et al. (2015) argues that IoT technologies have the ability to reach a full potential maximum estimated value of 11.1 USD trillion by 2025, a value that is equivalent to 11% of the world economy. The greatest source of economic value attained from the use of IoT technologies is expected to be seen in factories, more specifically in operations and predictive management. In addition to the latter, it is also argued that a strong economic impact will be derived from public safety and health, traffic control and resource management.

Since the foundation of IoT technologies relies heavily on the use of wireless autonomous device communication through wireless connectivity to various networks, this suggests that the further development these technologies will result in an exponential increase of device connectivity. The telecommunication industry will become a key player in this respect as data services, which are offered in subscription packages by telecommunication service providers are likely to see a consequent increase in demand. This increase in demand is fuelled by the rise in the number of internet-connected devices, which will cause an increase in the volume of subscriber-based consumers and traffic as further implementation of IoT technologies ensues in the economy.

As an increase in internet-connected devices arises, suppliers must increase production to match the subsequent increase in demand. It is therefore plausible to expect growth in the hardware manufacturing industry. The rise of IoT technologies also means the size of hardware, in particular that of microprocessors is getting smaller and more powerful potentially meaning a decrease in the costs of production of hardware (Charles Saidu 2015). In addition, from the supply side perspective, an increase in the number of firms supplying the market occurs. This decreases the market price as the number of firms supplying the hardware manufacturing market increases. Economic theory states that in the long-run, the market equilibrium is determined by market forces and is found at the point which market demand equals market supply.

The potential risks of IoT are rooted within its tremendous potential. The introduction and development of more advanced features imply the presence of greater security and privacy risks. Given this, adequate cybersecurity measures must be implemented to ensure immunity to the potential threats that will arise in the near future. This factor gains further emphasis due to the increased complexity of IoT technologies, which means there are greater device functions that must be secured (Greengard 2017). In addition, the risker the functionality present in the web-enabled devices, the greater the emphasis that must be placed on security. For usefulness to be maximised and risk to be minimised businesses and producers must work together to develop IoT technologies that are secure by default, allowing businesses to use them without endangering the privacy of stakeholders.

5. Conclusions

The current scientific foundation of *Enterprise Interoperability* has been lacking specific theories. Despite the abundance of theories in fields that are related in one way or another with 'Interoperability', there has been little progress in terms of developing Interoperability's own theories, although there is a clear identification of where such theories are required in order to improve EI.

Overall, there is worldwide significant applied research and technology development across most of the relevant enterprise system application domains. Nevertheless, a large scope for theory as far EI is concerned, and fundamental research effort in this area should be increased in order to have more systemantic and sustainable development of EI as a scientific discipline.

Acknowledgments

Project BG05M2OP001-1.002-0002 "Digitization of the economy in an environment of Big data", OP Science and Education for Smart Growth and the European Regional Development Fund.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Atzoria, L., A. Ierab, G. Morabitoc, and M. Nittia. 2012. "The Social Internet of Things (Siot) – When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization." *Computer Networks* 56 (16): 3594–3608. doi:10.1016/j.comnet.2012.07.010.

Cestari, J. M. A. P., E. D. F. Rocha-Loures, E. A. Portela-Santos, and P. Panetto. 2019. "A Capability Model for Public Administration Interoperability." *Enterprise Information Systems*. doi:10.1080/17517575.2018.1564154.

Charles Saidu, A. U. 2015. "Internet of Things: Impact on Economy." *British Journal of Mathematics & Computer Science* 7 (4): 241–251. doi:10.9734/BJMCS/2015/14742.

CISCO. 2013. "Introduction to the Internet of Everything At-A-Glance." http://www.cisco.com/web/about/ac79/docs/IoE/IoE-AAG.pdf

CMMI Product Team. 2010. *CMMI for Development, Version 1.3*. Pittsburgh: Software Engineering Institute. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9661

Creswell, J. W. 2014. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4th ed. Los Angeles: Sage Publications.

Davis, J. P., K. Eisenhardt, and B. C. Bingham 2007. "Complexity Theory, Market Dynamism and the Strategy of Simple Rules". In Proceedings of DRUID Summer Conference 2007 on Appropriability, Proximity Routines and Innovation, Copenhagen, CBS, Denmark, June 18–20.

Filippini, R. 1997. "Operations Management Research: Some Reflections on Evolution, Models and Empirical Studies in OM." *International Journal of Operations & Production Management* 17 (7): 655–670. doi:10.1108/01443579710175583.

Greengard, S. (2017). "Companies Struggle to Adopt IoT Security & Privacy". http://www.baselinemag.com/innovation/internet-of-things/companies-struggle-to-adopt-iot-security-privacy.html

Irfan Saif, S. P. 2015. *Safeguarding the Internet of Things: Being Secure, Vigilant, and Resilient in the Connected Age*. Deloitte University Press. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ra-safeguarding%20the%20IoT.pdf.

ISO/IEC. 2015. *Information Technology-Process Assessment-Concepts and Terminology*. Genève: International Organization for Standardization. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54175

Jardim-Goncalves, R., A. Grilo, and A. Steiger-Garcao. 2006a. "Challenging the Interoperability in the Construction Industry with MDA and SOA." *Computers in Industry* 57 (8–9): 679–689. doi:10.1016/j.compind.2006.04.013.

Jardim-Goncalves, R., A. Steiger-Garcao, and C. Agostinho 2010. "Sustainable Systems' Interoperability: A Reference Model for Seamless Networked Business". 2010 IEEE International Conference on Systems, Man and Cybernetics, Istanbul, pp. 1785–1792, 10.1109/ICSMC.2010.5642295.

Khisro, J., and H. Sundberg. 2018. "Enterprise Interoperability Development in Multi Relation Collaborations: Success Factors from the Danish Electricity Market." *Enterprise Information Systems* 1–22. doi:10.1080/17517575.2018.1528633.

Leng, J., P. Jiang, C. Liu, and C. Wang. 2018. "Contextual Self-Organizing of Manufacturing Process for Mass-Individualization: A Cyber-Physical-Social System Approach." *Enterprise Information Systems* 1–26. doi:10.1080/17517575.2018.1470259.

Lezoche, M., and H. Panetto. 2018. "Cyber-Physical Systems, A New Formal Paradigm to Model Redundancy and Resiliency." *Enterprise Information Systems* 1–22. doi:10.1080/17517575.2018.1536807.

Manyika, J., et al. 2015. *The Internet of Things: Mapping the Value beyond the Hype*. San Francisco: McKinsey Global Institute. https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.pdf

Martins, L., M. L. R. Varela, N. O. Fernandes, S. Carmo-Silva, and J. Machado. 2020. "Literature Review on Autonomous Production Control Methods." *Enterprise Information Systems* 1–13. doi:10.1080/17517575.2020.1731611.

Panetto, H., M. Zdravkovic, R. Jardim-Goncalves, D. Romero, J. Cecil, and I. Mezgár. 2015. "New Perspectives for the Future Interoperable Enterprise Systems." *Computers in Industry, Special Issue: Future Perspectives on Next Generation Enterprise Information Systems: Emerging Domains and Application Environments* 79: 47–63. doi:10.1016/j.compind.2015.08.001.

Princeton University. 2018. *WordNet [Lexical Database of English]*. New Jersey, USA: Princeton University. http://wordnet.princeton.edu

Romero, D., and F. Vernadat. 2015. "Enterprise Information Systems State of the Art: Past, Present and Future Trends." *Computers in Industry, Special Issue: Future Perspectives on Next Generation Enterprise Information Systems: Emerging Domains and Application Environments* 79: 3–13. doi:10.1016/j.compind.2016.03.001.

Sakellarios, A., J. Correia, S. Kyriakidis, E. Georga, N. Tachos, S. Siogkas, F. Sans, et al. 2020. "A Cloud-based Platform for the Non-Invasive Management of Coronary Artery Disease." *Enterprise Information Systems* 1–22. doi:10.1080/17517575.2020.1746975.

Toney, R. 2016. "Risk Management in the Internet of Things." *Enterprise Risk Management Initiative*. https://erm.ncsu.edu/library/article/risk-management-in-the-internet-of-things

Tsiouris, K. M., D. Gatsios, V. Tsakanikas, A. A. Pardalis, I. Kouris, T. Androutsou, M. Tarousi, et al. 2020. "Designing Interoperable Telehealth Platforms: Bridging IoT Devices with Cloud Infrastructures." *Enterprise Information Systems* 1–25. doi:10.1080/17517575.2020.1759146.

Yin, R. K. 2013. *Case Study Research: Design and Methods*. 5th ed. Los Angeles: Sage Publications.

Zhou, R., Y. Cao, R. Zhao, Q. Zhou, J. Shen, Q. Zhou, and H. Zhang. 2019. "A Novel Cloud-Based Auxiliary Medical System for Hypertension Management." *Applied Computing and Informatics* 15 (2): 114–119. doi:10.1016/j.aci.2017.10.002.

Ricardo Jardim-Goncalves
Uninova – Cts, Caparica, Portugal
rg@uninova.pt
Departamento Engenharia ELetrotecnica E Computadores, Faculdade De Ciencias E Tecnologia, Universidade NOVA De Lisboa, Caparica, Portugal http://orcid.org/0000-0002-3703-6854

David Romero
Tecnológico De Monterrey, Mexico City, Mexico

Diogo Goncalves
University of Saint Andrews, St Andrews, UK

João Pedro Mendonça
Departamento De Engenharia Mecânica, Universidade Do Minho, Guimaraes, Portugal
Translational Sciences, Sanofi, 640 memorial drive, Cambridge

Received 21 August 2020 accepted 21 August 2020