CCF Transactions on Pervasive Computing and Interaction (2021) 3:329–338
https://doi.org/10.1007/s42486-021-00057-3

REVIEW PAPER

Artificial Intelligence and the Internet of Things in Industry 4.0

Petar Radanliev[1] · David De Roure[1] · Razvan Nicolescu[2] · Michael Huth[3] · Omar Santos[4]

Received: 26 November 2020 / Accepted: 25 February 2021 / Published online: 16 March 2021

Abstract
This paper presents a new design for artificial intelligence in cyber-physical systems. We present a survey of principles, policies, design actions and key technologies for CPS, and discusses the state of art of the technology in a qualitative perspective. First, literature published between 2010 and 2021 is reviewed, and compared with the results of a qualitative empirical study that correlates world leading Industry 4.0 frameworks. Second, the study establishes the present and future techniques for increased automation in cyber-physical systems. We present the cybersecurity requirements as they are changing with the integration of artificial intelligence and internet of things in cyber-physical systems. The grounded theory methodology is applied for analysis and modelling the connections and interdependencies between edge components and automation in cyber-physical systems. In addition, the hierarchical cascading methodology is used in combination with the taxonomic classifications, to design a new integrated framework for future cyber-physical systems. The study looks at increased automation in cyber-physical systems from a technical and social level.

Keywords Industrial internet of things · Cyber-physical systems · Industry 4.0 · Artificial intelligence

1 Introduction

Artificial intelligence (AI) and the Internet of Things (IoT) are the driving forces for industrial automation and the concept of smart factory. The industrial automation is shofting towards predictive maintenance and quality, human–robot integrations, and adaptive supply chains. While the industrial world is slowly getting used to the Industry 4.0 idea, the world is already evolving in the industry 5.0 (Sarfraz et al. 2021). This study reviews a juxtaposition of related systems and technologies, including IoT; Industrial Internet of Things (IIoT); Cyber-physical systems (CPS); and Industry 4.0 (I4.0). We briefly explain these related systems and technologies. The IIoT represents an evolved and connected distributed control system, using sensor, and other connected devices for data collection, exchange and analysis for improved productivity, energy management and other economic benefits (Boyes et al. 2018). The I4.0 is a generic designation for sets of strategic frameworks and initiatives, and a technical term to relate to new emerging digitalisation of business assets, processes and services. Different terms are used depending on the country, but all represent the same idea, which is '*The Fourth Industrial Revolution*' (Carruthers 2016).

The IoT represents many different connected devices, using different connection protocols, performing data collection, for cloud storage, real-time analytics, among many other functions that create value (Nicolescu et al. 2018). On the other hand, the term CPS represents 'smart' systems that are built and depend on the interaction between physical and computational components (Craggs and Rashid

✉ Petar Radanliev
petar.radanliev@eng.ox.ac.uk

David De Roure
david.de.roure@oerc.ox.ac.uk

Razvan Nicolescu
rn@ucl.ac.uk

Michael Huth
m.h.m@imperial.ac.uk

Omar Santos
m.ontalvo@cisco.com

1 Oxford E-Research Centre, Engineering Science Department, University of Oxford, 7 Keble Road, Oxford OX1 3QG, England

2 Department of Anthropology, University College London, London, England, UK

3 Department of Computing, Imperial College London, London, England, UK

4 Cisco Research Centre, Research Triangle Park, NC, USA

2017). CPS emerges from the interconnection of physical components in complex software to form new network and systems capabilities. While IoT focuses on interconnectivity, interoperability and integration of physical components in the Internet. Integration of IoT and CPS is what defined the IIoT and is expected to lead to developments of I4.0 in automation, real-time platforms, and automation guiding workers in production environment.

The research questions this study investigates are related to identifying the networked connection of people, processes, data, and things. The study is investigating the concepts that unites the cyber-physical world with the social aspects of the environment in which this technology is deployed. Also, a crucial question of interest for the study, is to review all available resources and identify the future cognitive makeup of I4.0. The terms 'artificial intelligence', 'artificial cognition', 'cognition', and 'cognitive CPS', in the context of this article are used interchangeably. These terms cohere to existing literature discussion on the effect from the evolving coupled systems and social networks in interconnected industrial systems. This article discusses major new initiatives in the industrial and manufacturing space in relation to privacy preserving and cyber risks in cyber-physical systems.

2 Cyber-physical systems in Industry 4.0

The engagement of AI in the cyber world and the human engagements in the physical world have been studied excessively in isolation, but the roadmap to I4.0 is still unclear (Caiado et al. 2021) and little attention has been given to the combination of AI and the cyber-physical world (Hollebeek et al. 2021). The world leading Industry 4.0 frameworks (Table 1)—identified from (Radanliev et al. 2020a, b, c, d, e) are analysed in a (a) comparative empirical study that correlates (b) hierarchical cascading based on the (c) grounded theory approach to determine (d) taxonomic classifications. A comparative empirical study (Murray-Rust et al. 2014; Van Kleek et al. 2018) is used to establish a design process (Lee et al. 2019a, 2019b) for integrating present CPS techniques and literature review for the future CPS techniques in Industry 4.0.

The results of the comparative empirical study on Industry 4.0 frameworks, are presented in detail in (Figure, Figure, and Figure) to determine the present and future mechanisms for artificial intelligence automation in cyber-physical systems. The complete findings of the comparative empirical study, correlated with hierarchical cascading of the taxonomic classifications from the grounded theory method, are presented in the Figure. The integrated framework in Figure compensates for shortcomings in each of the individual frameworks reviewed, calling for a standardised framework (Radanliev et al. 2020). For example, not all frameworks provide mechanisms for policy development.

Hence, our architecture (in Figs. 1 and 2) derives integrated recommendations and mechanisms that are directly related to increasing cognition in CPS. The methodology for designing our architecture (in Figs. 1 and 2) is related to from proof-of-concept (Wang et al, 2019), graph based visual analysis (Böhm et al. 2018), for ensuring data confidentiality (Zhang et al. 2018).

The architecture framework in Figure makes direct recommendations for elements of action, through integrating best practices from the empirical analysis. Figure integrates taxonomic grouping techniques (Figure node 1:1) from academic literature, to establish the CPS integration framework (in Figure node 1.2), with practical initiatives (in Figure node 1:3) from empirical studies data and consolidates these techniques with a cascading framework (in Figure node 1.4) that relates artificial intelligence with CPS technologies. A taxonomic grouping of future and present techniques is conceptualised with existing hierarchical cascading design (Radanliev 2016). By doing this, the leading initiatives are

Table 1 Industry 4.0 national frameworks

Industry 4.0 frameworks
Germany—Industrie 4.0
USA—(1) Industrial Internet Consortium; (2) Advanced Manufacturing Partnership
UK—(3) Digital Catapults; (4) UK Digital Strategy; (5) Made Smarter
Japan—(6) Industrial Value Chain Initiative (IVI, 2017); (7) New Robot Strategy (NRS) and (8) RRI
France—(9) New France Industrial (NFI)
Nederland—(10) Smart Industry
Belgium—(11) Made Different
Spain—(12) Industrie Conectada 4.0
Italy—(13) Fabbrica Intelligente
China—(14) Made in China 2025
G20—(15) New Industrial Revolution (NIR)
Russia—(16) National Technology Initiative (NTI)

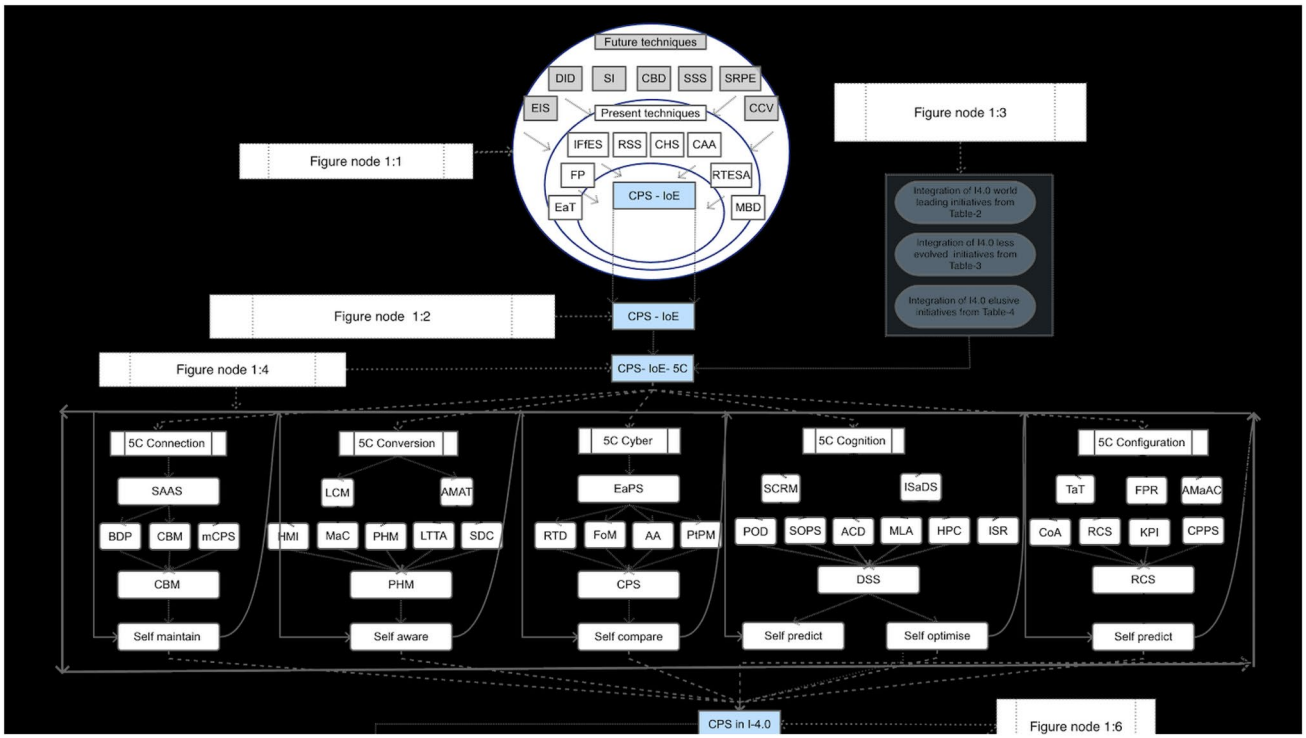

Fig. 1 Architecture for future cyber-physical systems

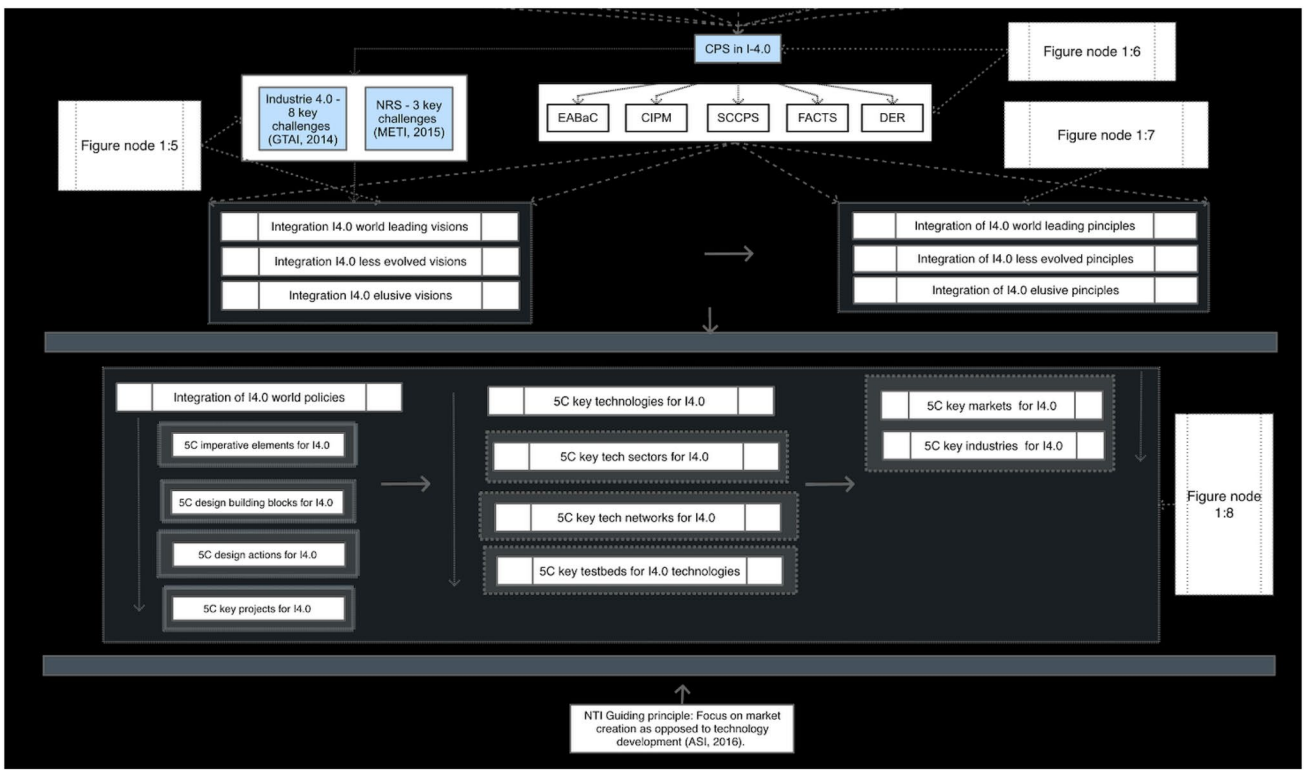

Fig. 2 Direction of the logical flow of cognitive CPS design

aggregated in integration areas. The integration framework in Figure follows taxonomic approach, in the formulation of encompassing principles for the integration across all initiatives (Figure node 1:3).

The argument of this process is that the integration of artificial cognition in CPS is not a selective process. Rather, it requires the synchronisation and harmonisation, which requires evaluation principles. The first stage of this study identified the related elements and principles from academic literature. These are grouped (from Figure nodes 1.1, to 1.4) and combined with present and future challenges from recent literature. To avoid duplication of abbreviations, the figure node 1:4 and the full list of abbreviations are borrowed from (Radanliev et al. 2020). The remaining Figure nodes emerge from this study. This presents the state-of-the-art in current understanding on the integration of artificial cognition in CPS. The arrows in Figs. 1 and 2, stand for the direction of the logical flow of cognitive CPS design.

In the second stage (Figure nodes 1.6 to 1.8), the hierarchical cascading process is shaped by practical initiatives. In the hierarchical cascading we designed, there is a reflexion on the knowledge that a supply chain view is necessary for obtaining the industry 4.0 values, and that organisations need to first integrate culturally in the industry 4.0 concept, before the supply chain is digitalised, and the implementation needs to be a phased approach (Shao et al. 2021). These postulates are integral part of the architecture we designed in Fig. 1, and are based on the knowledge that the main values of industry 4.0 is in the supply chain (Fatorachian and Kazemi 2021).

The empirical study builds upon the Figs. 1 and 2 and is presented in Figs. 3, 4, 5, 6, 7, where Fig. 3 analyses the integration aspect (vision and principles) of all practical initiatives in the empirical study (building upon the concept from Figure node 1.5).

The Figure details the results of the comparative empirical study on Industry 4.0 frameworks, to determine the present mechanisms for artificial intelligence automation in cyber-physical systems. The empirical study considers CPS as similar to social machines (Mons 2019), with perceived moral scale (Banks 2019), for algorithmic regulation (Radanliev et al. 2020). This connection was based on the notion that social machines and the IoT are interrelated (Smart et al. 2019), and we found the archetypal narrative (Tarte et al. 2015) in observing the social aspect (De Roure et al. 2015) of CPS's, for the emergence of a cyber-physical social machine (Madaan et al. 2018). In Figure, we use this approach to identify the hierarchy of the taxonomy from the comparative empirical study. This results with a cascading hierarchy (Figure) for integration policies based on imperative elements, design building blocks, design

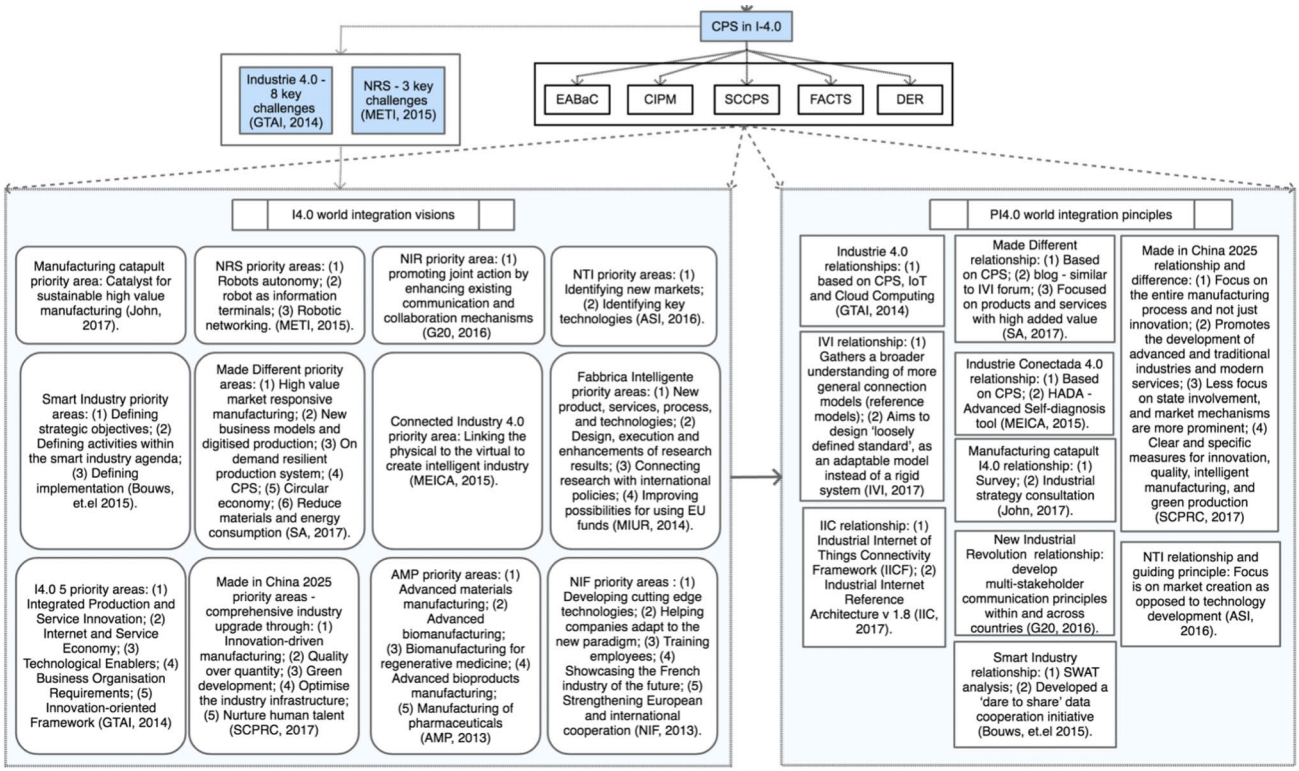

Fig. 3 Principles for cyber-physical systems in Industry 4.0

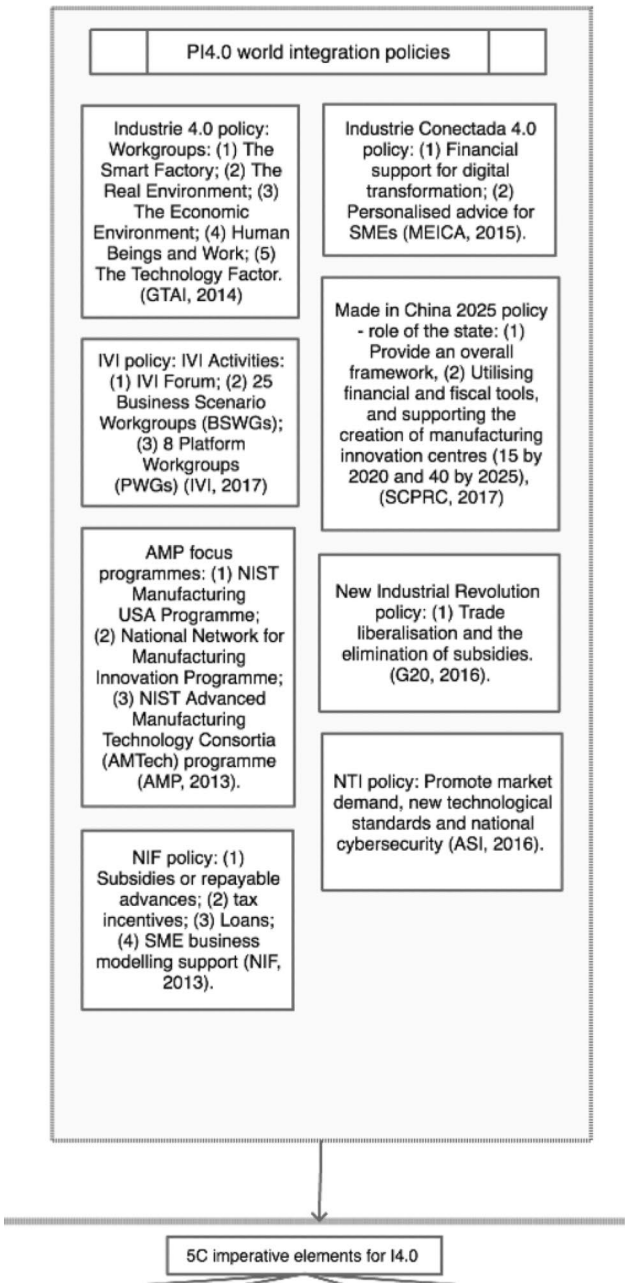

Fig. 4 CPS policies

actions, and key projects for the design and prototype of AI-enabled cyber-physical systems.

Building upon the cascading hierarchy in Figure, in Figure the same methodology was applied to derive the key technologies, key tech sectors, key tech networks, key testbeds, key industries and markets and guiding principles, for the design and prototype of AI-enabled cyber-physical systems. This cascading hierarchy mechanism is the result of a conceptual method to integrate the I4.0 initiatives into a logical sequence of cognition. The design follows findings that such integrations must consider the value created, while focusing on understanding the risk, including future risks. Most peculiar finding from the empirical study is that apart from the Japanese NRS and RRI, all other world initiatives have failed to provide clarification on how artificial intelligence (AI) would be integrated in their I4.0 strategies. The cognitive feedback mechanism provides a logical sequence that includes the NRS core technologies specification for the integration of AI and automated behaviour in the NFI key technologies list. While with the evolution of other elements will emerge, in Figure node 1.8, the current building blocks for artificial cognition in CPS are extracted from the requirements of the imperative elements as presented in the leading initiatives and policies for reducing the associated cyber risk.

The imperative elements (in Figure node 1:8) are followed by the design building blocks. The design building blocks represent more specific concepts and can serve as guidance and feedback mechanisms for the future artificial cognition in CPS. Building block concepts, such as: information transparency and open access facilities provide guidance to national regulators and industry network architects. The process provides feedback mechanisms from national strategies towards standardisation strategy. For example, one feedback mechanism could be the NTI's initiative to build a block for electronic open submission of recommendations for changing or editing. Some of the building blocks seem conflicting, e.g. loosely defined standards vs. standardisation. The reason is that I4.0 is continuously evolving, and standardisation must accommodate for changes as this evolution occurs. This situation is very different from the incumbent industries, where standardisation normally refers to a fixed set of rules and regulations within a well-defined domain. In the cyber world, standardisation needs to be adaptive, hence the process of standardisations must anticipate constant future changes. This process includes a certain initial degree of continually evolving loosely-defined standardisation.

3 Discussion: alternative testing and validation of the framework

Research on CPS requires development of testbeds to validate the proposed solutions (Hahn et al. 2013). Some elements of cognition in CPS are still futuristic and require virtual validation in the design stages (Leitão et al. 2016). In different types of CPS (ex. autonomous vehicles) the futuristic elements discussed have already been applied. Examples include virtual evaluation, validation and design platforms (Feth et al. 2015), unmanned network navigation and autonomous navigation (Berger and Rumpe 2014), context aware CPS with Cloud Support (Wan et al. 2014),

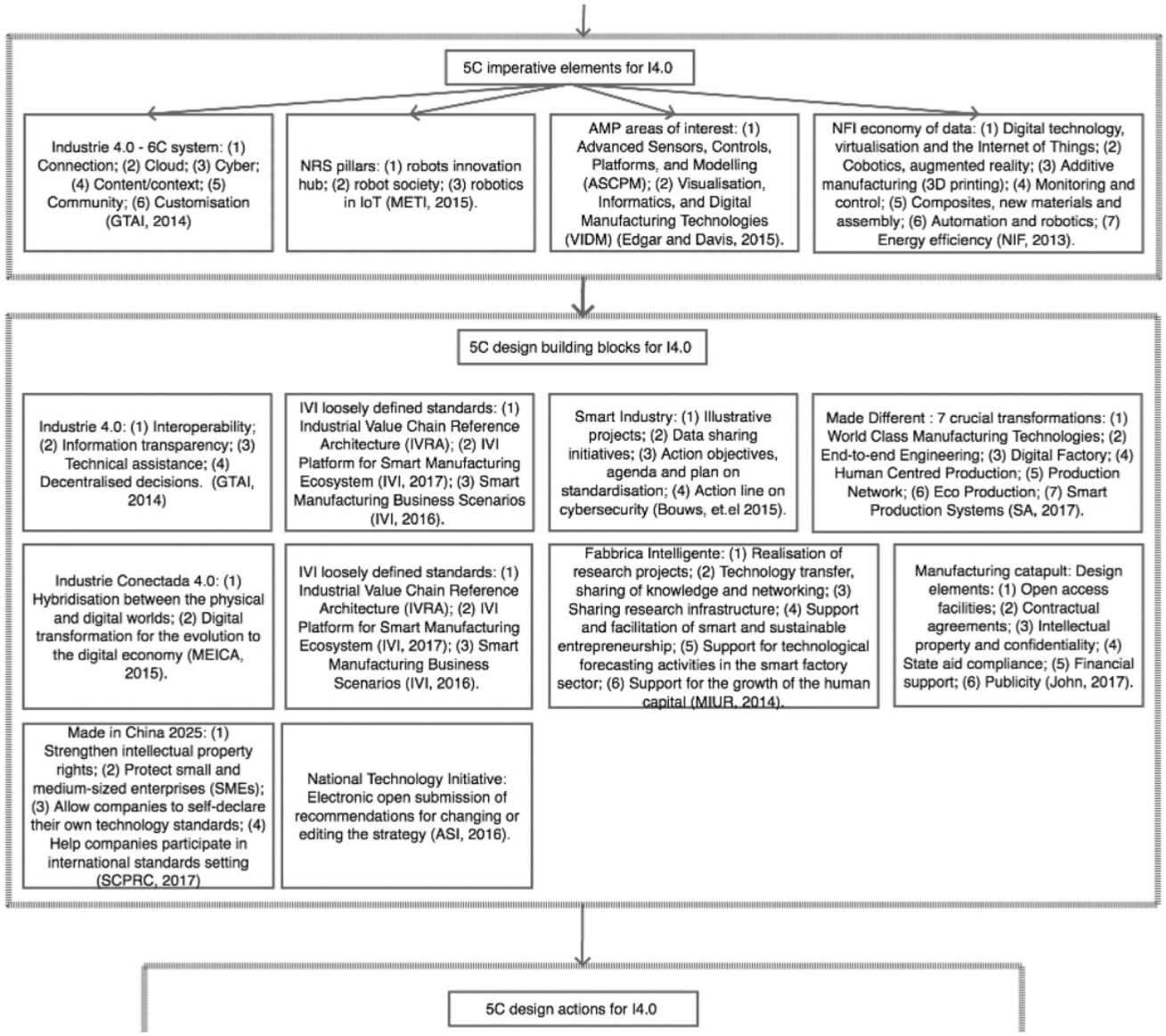

Fig. 5 CPS elements and building blocks

autonomous energy management and integration of CPS in the cloud (Radanliev et al. 2020). The verification problem of the architecture model in this study could be attempted for example through fuzzy verification that involves a sequence of Boolean questions and decisions meant to provide a level of confidence for a correct implementation of specific elements. But this verification would hardly provide a reasonable level of confidence for various systems of systems let alone for the entire system, also because some of the technologies discussed are not even invented, such as AI brain (Ministry of Economy Trade and Industry of Japan 2015). Alternatively, industrial developers can test the framework by applying object oriented layered architecture for the cyber–physical components (Thramboulidis 2015). However, to introduce performance measurements, this method over-simplifies the process. Continuous experimentation method can also be applied in automated virtual testing, using simulations and data recordings from CPS (Giaimo et al. 2016). However, this method presents serious weaknesses in terms of safety guarantees, hardware constraints and lack of supportive instruments.

4 Conclusions

The framework identifies significant advancements in the past 10 years, that are missing the individual framework analysed in the literature survey. For example, in current

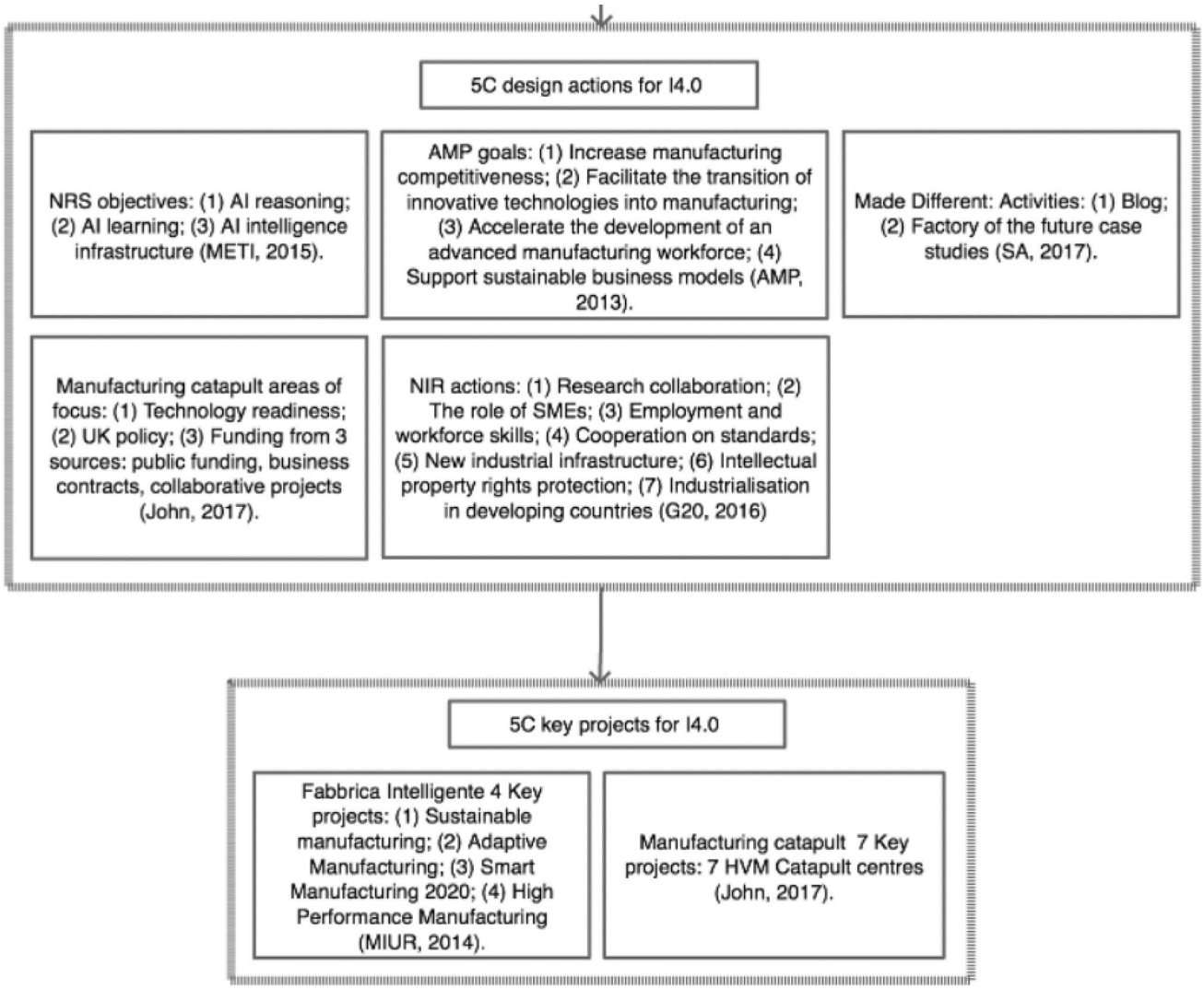

Fig. 6 CPS design actions

literature AI in CPS is represented only as simple decision support system, with a single focus on manufacturing processes. These capabilities can, and have been achieved in various ways that are not related to AI. The new framework presented in this review paper, integrates AI with much more than a simple decision support system, touching upon areas in social machines, connected devices, knowledge developments, among new cognitive concepts, emerging from individual Industry 4.0 frameworks. The complexities of cognitive automation are organised in a hierarchical cascading structure in the new integration framework, enabling the management of collaborative systems safely and securely while using resources efficiently.

This paper presents a future vision for AI evolution in cognitive automation mechanisms, based on AI-enabled cyber-physical systems. The paper also identifies a methodological design for specific challenges, such as AI in I4.0. The framework produces a taxonomy of common basic terminology, common approaches, and existing world leading initiatives into a proposition of AI-enabled cyber-physical systems. The review paper also suggests the need to formulate compositional ways to reason about the emerging cyber risks in an CPS context. The framework enables the current efforts to integrate in a larger perspective, in the development of cyber policy.

Finally, the contribution of this paper is two-fold. Firstly, the paper developed a method for aggregating evidence on the emerging advancements in the field of cognitive mechanisms for design and prototype of AI-enabled cyber-physical systems. The review paper combines approaches to incorporate existing standards into new design for cognition in CPS. Secondly, the paper captures some of the best practices in industry and develops a step-by-step process design and prototype of AI-enabled cyber-physical systems. The new framework can

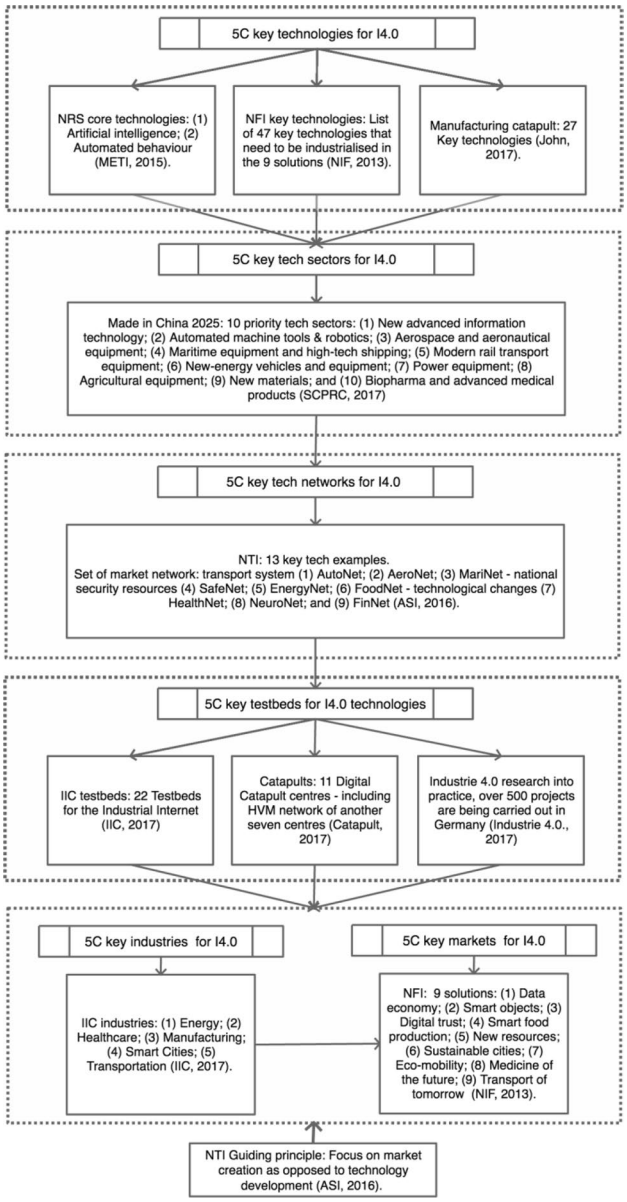

Fig. 7 Key technologies, key tech sectors, key tech networks, key testbeds, key industries and markets and guiding principles

be used by governments for improving existing national strategies, or designing new national strategy, especially by developing countries. The framework can also be used as guidance in cyber policy design for AI-enabled cyber-physical systems. Private sector enterprises can use the framework for determining future changes in national strategy and policies.

5 Limitations of this study

Future research should give consideration of system sociology because the conceptual model presented does not address the question of skilled job losses. The study accepted the argument that the associated social disruptions will be significant as the technologically driven labour market transitions are likely to take considerable time, especially in situations when AI accelerates the pace of automation. The study accepted the counter argument is that skilled and educated jobs will be created to control and maintain machines, as automation optimises the manufacturing competitive edge in high-wage countries (Brettel et al. 2016), and enables a better work-life-balance in a high-wage economy. We believe that elements in this article would contribute to the ongoing debates on the two opposing viewpoints.

Acknowledgements Eternal gratitude to the Fulbright Visiting Scholar Programme.

Authors' contributions PR: main author; DR: supervision; RN, MH, OS supervision, review and corrections.

Funding This work was funded by the UK EPSRC [Grant Number: EP/S035362/1] and by the Cisco Research Centre [grant number DFR05640].

Availability of data and material N/A—all data and materials included in the article text.

References

Banks, J.: A perceived moral agency scale: development and validation of a metric for humans and social machines. Comput. Hum. Behav. **90**, 363–371 (2019). https://doi.org/10.1016/j.chb.2018.08.028

Berger, C., & Rumpe, B. (2014). Autonomous driving—5 years after the urban challenge: the anticipatory vehicle as a cyber-physical system. http://arxiv.org/abs/1409.0413

Böhm, F., Menges, F., Pernul, G.: Graph-based visual analytics for cyber threat intelligence. Cybersecurity **1**(1), 1–19 (2018). https://doi.org/10.1186/s42400-018-0017-4

Boyes, H., Hallaq, B., Cunningham, J., Watson, T.: The industrial internet of things (IIoT): an analysis framework. Comput. Ind. **101**, 1–12 (2018). https://doi.org/10.1016/J.COMPIND.2018.04.015

Brettel, M., Fischer, F.G., Bendig, D., Weber, A.R., Wolff, B.: Enablers for self-optimizing production systems in the context of industrie 4.0. Procedia CIRP **41**, 93–98 (2016). https://doi.org/10.1016/j.procir.2015.12.065

Caiado, R.G.G., Scavarda, L.F., Gavião, L.O., Ivson, P., de Nascimento, D.L., M., & Garza-Reyes, J. A. : A fuzzy rule-based industry 4.0

maturity model for operations and supply chain management. Int. J. Prod. Econ. **231**, 107883 (2021). https://doi.org/10.1016/j.ijpe.2020.107883

Carruthers, K. (2016). Internet of Things and Beyond: Cyber-Physical Systems—IEEE Internet of Things. IEEE Internet of Things. http://iot.ieee.org/newsletter/may-2016/internet-of-things-and-beyond-cyber-physical-systems.html

Craggs, B., & Rashid, A. (2017). Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design. *2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, 22–25. https://doi.org/https://doi.org/10.1109/SEsCPS.2017.5

De Roure, D., Hooper, C., Page, K., Tarte, S., & Willcox, P. (2015). Observing social machines part 2: How to observe? *Proceedings of the 2015 ACM Web Science Conference*, 1–5. https://doi.org/https://doi.org/10.1145/2786451.2786475

Fatorachian, H., Kazemi, H.: Impact of Industry 4.0 on supply chain performance. Prod. Plann. Control **32**(1), 63–81 (2021). https://doi.org/10.1080/09537287.2020.1712487

Feth, P., Bauer, T., & Kuhn, T. (2015). Virtual Validation of Cyber Physical Systems. *Software Engineering & Management*. http://cs.emis.de/LNI/Proceedings/Proceedings239/201.pdf

Giaimo, F., Yin, H., Berger, C., & Crnkovic, I. (2016). Continuous Experimentation on Cyber-Physical Systems. *Proceedings of the Scientific Workshop Proceedings of XP2016 on - XP '16 Workshops*, 1–2. https://doi.org/https://doi.org/10.1145/2962695.2962709

Hahn, A., Ashok, A., Sridhar, S., Govindarasu, M.: Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans. Smart Grid **4**(2), 847–855 (2013). https://doi.org/10.1109/TSG.2012.2226919

Hollebeek, L.D., Sprott, D.E., Brady, M.K.: Rise of the machines? Customer engagement in automated service interactions. J. Service Res. **24**(1), 3–8 (2021). https://doi.org/10.1177/1094670520975110

Lee, B., Cooper, R., Hands, D., & Coulton, P. (2019a). Design Drivers: A critical enabler to meditate value over the NPD process within Internet of Things. *4d Conference Proceedings: Meanings of Design in the Next Era. Osaka : DML (Design Management Lab), Ritsumeikan University*, 96–107.

Lee, B., Cooper, R., Hands, D., & Coulton, P. (2019b). Value creation for IoT: Challenges and opportunities within the design and development process. *Living in the Internet of Things (IoT 2019). IET, Living in the Internet of Things 2019, London, United Kingdom*, 1–8. https://doi.org/https://doi.org/10.1049/cp.2019.0127

Leitão, P., Colombo, A.W., Karnouskos, S.: Industrial automation based on cyber-physical systems technologies: prototype implementations and challenges. Comput. Ind. **81**, 11–25 (2016). https://doi.org/10.1016/j.compind.2015.08.004

Madaan, A., Nurse, J., de Roure, D., O'Hara, K., Hall, W., Creese, S.: A storm in an IoT cup: the emergence of cyber-physical social machines. SSRN Electronic Journal (2018). https://doi.org/10.2139/ssrn.3250383

Ministry of Economy Trade and Industry of Japan. (2015). *NRS, New Robot Strategy—Vision Strategy and Action Plan; Ministry of Economy Trade and Industry of Japan*. http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf

Mons, B.: FAIR science for social machines: let's share metadata knowlets in the internet of FAIR data and services. Data Intelligence **1**(1), 22–42 (2019). https://doi.org/10.1162/dint_a_00002

Murray-Rust, D., Van Kleek, M., Dragan, L., & Shadbolt, N. (2014). Social palimpsests - clouding the lens of the personal panopticon. *Digital Enlightenment Yearbook*, 75–97. https://eprints.soton.ac.uk/372125/

Nicolescu, R., Huth, M., Radanliev, P., De Roure, D.: Mapping the values of IoT. J. Inf. Technol. **33**(4), 345–360 (2018). https://doi.org/10.1057/s41265-018-0054-1

Radanliev, P. (2016). Supply chain systems architecture and engineering design: green-field supply chain integration. *Operations and Supply Chain Management 9*:1. https://doi.org/https://doi.org/10.20944/preprints201904.0122.v1

Radanliev, P., De Roure, D., Nurse, J.R.C., Mantilla Montalvo, R., Cannady, S., Santos, O., Maddox, L., Burnap, P., Maple, C.: Future developments in standardisation of cyber risk in the Internet of Things (IoT). SN Appl Sci **2**(2), 1–16 (2020). https://doi.org/10.1007/s42452-019-1931-0

Radanliev, P., De Roure, D., Van Kleek, M., Ani, U., Burnap, P., Anthi, E., Nurse, J.R.C., Santos, O., Montalvo, R.M., Maddox, L.T.: Dynamic real-time risk analytics of uncontrollable states in complex internet of things systems: cyber risk at the edge. Environ. Syst. Decis. **1**, 1–12 (2020). https://doi.org/10.1007/s10669-020-09792-x

Radanliev, P., De Roure, D., Van Kleek, M., Santos, O., Ani, U.: Artificial intelligence in cyber physical systems. AI Soc. **1**, 1–14 (2020). https://doi.org/10.1007/s00146-020-01049-0

Radanliev, P., De Roure, D., Walton, R., Van Kleek, M., Montalvo, R.M., Maddox, L., Santos, O., Burnap, P., Anthi, E.: Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. SN Appl. Sci. **2**(11), 1–8 (2020). https://doi.org/10.1007/s42452-020-03559-4

Radanliev, P., Roure, D.. De., Page, K., Nurse, J.R.C., Montalvo, R.M., Santos, O., Maddox, L., Burnap, P.: Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 40 supply chains. Cybersecurity **3**(13), 1–21 (2020). https://doi.org/10.1186/s42400-020-00052-8

Sarfraz, Z., Sarfraz, A., Iftikar, H. M., & Akhund, R. (2021). Is COVID-19 pushing us to the Fifth Industrial Revolution (Society 5.0)? *Pakistan Journal of Medical Sciences*, *37*:2. https://doi.org/https://doi.org/10.12669/pjms.37.2.3387

Shao, X.F., Liu, W., Li, Y., Chaudhry, H.R., Yue, X.G.: Multistage implementation framework for smart supply chain management under industry 40. Technol. Forecast. Social Change **162**, 120354 (2021). https://doi.org/10.1016/j.techfore.2020.120354

Smart, P., Madaan, A., Hall, W.: Where the smart things are: social machines and the Internet of Things. Phenomenol. Cogn. Sci. **18**(3), 551–575 (2019). https://doi.org/10.1007/s11097-018-9583-x

Tarte, S., Willcox, P., Glaser, H., & De Roure, D. (2015). Archetypal narratives in social machines: Approaching sociality through prosopography. In: *Proceedings of the 2015 ACM Web Science Conference*, 1–10. https://doi.org/https://doi.org/10.1145/2786451.2786471

Thramboulidis, K.: A cyber–physical system-based approach for industrial automation systems. Comput. Ind. **72**, 92–102 (2015). https://doi.org/10.1016/j.compind.2015.04.006

Van Kleek, M., Binns, R., Zhao, J., Slack, A., Lee, S., Ottewell, D., & Shadbolt, N. (2018). X-Ray Refine. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–13. https://doi.org/https://doi.org/10.1145/3173574.3173967

Wan, J., Zhang, D., Sun, Y., Lin, K., Zou, C., Cai, H.: VCMIA: a novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing. Mobile Netw. Appl. **19**(2), 153–160 (2014). https://doi.org/10.1007/s11036-014-0499-6

Wang, Y., Wu, W., Zhang, C., Xing, X., Gong, X., Zou, W.: From proof-of-concept to exploitable. Cybersecurity **2**(1), 1–25 (2019). https://doi.org/10.1186/s42400-019-0028-9

Zhang, Q., Jia, S., Chang, B., Chen, B.: Ensuring data confidentiality via plausibly deniable encryption and secure deletion – a survey. Cybersecurity **1**(1), 1–20 (2018). https://doi.org/10.1186/s42400-018-0005-8

Petar Radanliev is a Post-Doctoral Research Associate at the University of Oxford. He obtained his Ph.D at University of Wales in 2014 and continued with Postdoctoral research at Imperial College London, Massachusetts Institute of Technology, University of Cambridge and University of Oxford. His current research focusses on artificial intelligence, internet of things, and cyber risk analytics at the edge.

David De Roure is a Professor of e-Research at University of Oxford. He obtained his PhD at University of Southampton in 1990 and went on to hold the post of Professor of Computer Science, later directing the UK Digital Social Research programme. His current research focusses on social machines, Internet of Things and cybersecurity. He is a Fellow of the British Computer Society and the Institute of Mathematics and its Applications.

Razvan Nicolescu is a digital anthropologist with an interest in understanding the social impact of new information and communication technologies. His research focuses on the relation between digital technology and political economy, ideology, governance, social change, social and economic inequality, normativity, feelings and ideals.

Michael Huth is a Professor of Computer Science in the Department of Computing, Imperial College London. His research focuses on Cybersecurity, Cryptography, Mathematical Modeling, and Formal Verification with applications in Machine Learning, FinTech, and Internet of Things.

Omar Santos is a Principal Engineer at Cisco Systems and an active member of the cyber security community, where he leads several industry-wide initiatives and standards bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of their critical infrastructures.