Article

New developments in Cyber Physical Systems, the Internet of Things and the Digital Economy – discussion on future developments in the Industrial Internet of Things and Industry 4.0

Petar Radanliev[1], David Charles De Roure[1], Jason R.C. Nurse[2], Razvan Nicolescu[3], Michael Huth[3], Stacy Cannady[4], Rafael Mantilla Montalvo[4]

1 [1]Oxford e-Research Centre, Department of Engineering Sciences, University of Oxford, UK, petar.radanliev@oerc.ox.ac.uk; david.deroure@oerc.ox.ac.uk;
2 [2]School of Computing, University of Kent, UK, j.r.c.nurse@kent.ac.uk;
3 [3] Imperial College London, UK, r.nicolescu@imperial.ac.uk, m.huth@imperial.ac.uk;
4 [4] Cisco Research Centre, Research Triangle Park, USA, scannady@cisco.com, montalvo@cisco.com

* **Corresponding author: Petar Radanliev: petar.radanliev@oerc.ox.ac.uk[1]**

Abstract: The world is currently experiencing the fourth industrial revolution driven by the newest wave of digitisation in the manufacturing sector. The term Industry 4.0 (I4.0) represents at the same time: a paradigm shift in industrial production, a generic designation for sets of strategic initiatives to boost national industries, a technical term to relate to new emerging business assets, processes and services, and a brand to mark a very particular historical and social period. I4.0 is also referred to as Industrie 4.0 the New Industrial France, the Industrial Internet, the Fourth Industrial Revolution and the digital economy. These terms are used interchangeably in this text. The aim of this article is to discuss major developments in this space in relation to the integration of new developments of IoT and cyber physical systems in the digital economy, to better understand cyber risks and economic value and risk impact. The objective of the paper is to map the current evolution and its associated cyber risks for the digital economy sector and to discuss the future developments in the Industrial Internet of Things and Industry 4.0.

Keywords: Internet of Things; Cyber Physical Systems; Digital Economy; Industrial Internet of Things; Industry 4.0; empirical analysis; cyber risk assessment; cyber risk target state

1 Introduction

The spectacular advancements in cyber physical systems (CPS) and Internet of Things (IoT) technology represent the foundation for the digital economy [1], the Industrial Internet of Things [2] and the Industry 4.0 [3]. The IoT term originated in 1999 along with the first view of how an IoT-based environment might look like in the future. On the other hand, the term CPS encompasses the complex and multi-disciplinary aspects of 'smart' systems that are built and depend on the interaction between physical and computational components. CPS theory emerges from control theory and control systems engineering and focuses on interconnection of physical components and use of complex software entities that establish new network and systems capabilities. CPS's thus link the physical and engineered systems and bridge the cyber world with the physical world. In contrast, IoT theory emerges from computer science and internet technologies and focuses on interconnectivity, interoperability and integration of physical components in the Internet. Integration work that would lead to developments such as IoT automation of CPS, real-time enabled CPS platforms, and automated CPS to guide skilled workers in production environment, is anticipated with the full IoT market adoption over the next decade.

The research reported here has two research objectives. Firstly, we present an up-to-date overview of existing and emerging advancements in the digital economy. Secondly, we capture the best practices in industry and offer a new theoretical model regarding harnessing the values from future developments in the digital economy. The model represents a reference architecture that enables the visualisation of network cyber risk, the minimization of IoT cyber risk, and the integration of the digital economy into what we refer to as a social machine. This reference architecture model can serve as a best practice and inform initial steps taken by organisations and governments in the digital economy space.

2 Methodology

The methods applied in this study consist of a cascading model [4]–[6] followed by a conceptual model development. As the landscape of IoT develops and changes very quickly – merely relying on journal publications provides too narrow a view of the present situation. We used the analytical target cascading [7], combined with the grounded theory approach [8], [9] in order to construct a conceptual [10] and cascading model [4], [11] for the evolution of cyber physical systems from IoT into the digital economy in a form of a social machine. These models then inform the new architectural reference model for the future developments in the digital economy.

3 Economic impact on the digital economy from new technologies

The exact economic impact of CPS and IoT infrastructure still remains to be determined [12], [13]. Since these technologies are already operational on a large scale in the digital economy, this situation requires a new model that provides an overall understanding of the design, development, and evolution of these technologies. Such model needs to integrate theories of IoT, control of physical systems, as well as their interaction with humans. This is the brief explanation of the connection we are making between the digital economy and social machines. The digital economy is connected and can process data in real-time. Such data input is collected from machines and humans and can be seen as digital assets with economical value [13], [14]. But such connected digital economy that represents a social machine, comes with cyber risks that we do not completely understand [15], [16] and we do not yet have the data to perform risk assessment [6], [17], [18].

There is an inherent risk in integrating the physical with the cyber world. Since we already defined that the digital economy operates as a social machine, the risk impact assessment should also change into cyber-financial assessment [19]. This requires an understanding of the digital economy network and the new cyber-financial risk elements also need to be quantified, such as intellectual property of digital information [13]. Cyber risk covers more elements than information security financial cost [6], [7], [17], [20]–[24], such as the intellectual property of digital assets [25]. Since there is no database and nobody has collected data until present to perform cyber-financial risk assessment of cyber risk from new technologies, the objective of this paper is to define the data collection parameters. This would enable governmental agencies to collect the correct data and will prevent a large data collection effort without the certainty of what data is needed and what data is not required.

4 Taxonomy of management methodologies for the digital economy

This section defines the reference architecture and creates a taxonomy representing a list of focal points for visualising and focusing the digital economy direction in the context of a social machine.

To define the term social machine in reference to the digital economy, we first explain the existing understanding of digital economy architecture (in Figure 1).

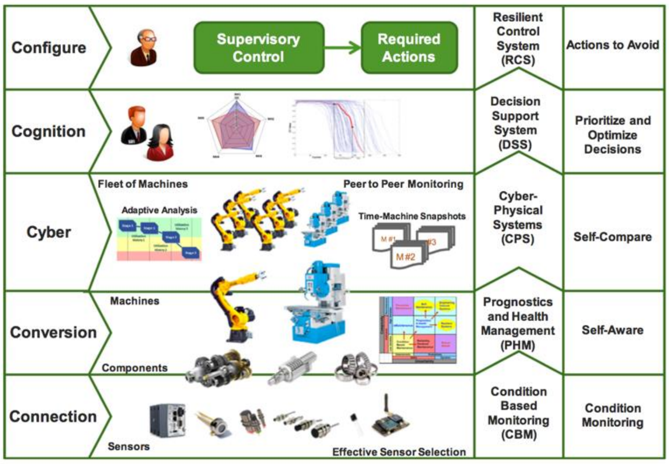

Figure 1: Current understanding of the digital economy [26]

The integration of artificial intelligence (AI), machine learning, the cloud, and IoT creates systems of machines capable of interacting with humans [3], [27]. The digital economy already has the capabilities for market speculation on human behaviour [3] and can determine consumer purchasing behaviour [7]. We can expect autonomous machines in the digital economy to start adopting the use of these methods in order to predetermine human behaviour. The digital economy brings together people, process, data, and things – making networked connections and transactions more valuable to individuals, organisations, and things. Hence, the key management technologies require (a) integration of physical flows, information flows, and financial flows; (b) innovative approaches to managing operational processes; (c) exploiting the IoT and industrial digitisation to gain competitiveness; (d) and utilisation of Big Data to improve the efficiency of production and services. These requirements are analysed and categorised in Table 1. The grounded theory method [8] is applied for the categorisation.

Categories of key elements for the digital economy to operate as a social machine	
Digital communities	
Cyber Physical Systems	CPS
Internet of Everything	IoE
5 level CPS architecture	5C
Agent-oriented Architecture	AoA
Object-oriented Architecture	OoA
Cloud optimised Virtual Object Architecture	VOA
Virtual Engineering Objects	VEO
Virtual Engineering Processes	VEP
Model-driven manufacturing systems	MDMS
Service oriented architecture	SoA
Dynamic intelligent swamps	DIS
Digital processes	
Connected devices and networks	CDN
Compiling for advanced analytics	CfAA
Business processes and services	BPS
Cloud distributed process planning	DPP
Physical and human networks	PHN
Digital societies	
Internet of Things	IoT

Web of Things	WoT
Social manufacturing	SM
Internet of People	IoP
Internet of Services	IoS
Systems of systems	SoS
Digital platforms	
Internet Protocol version 6	IPv6
Internet-based system and service platforms	ISP
Model-based development platforms	MBDP
Knowledge development and applications	KDoA
Real-time distribution	RtD

Table 1: New understanding of the digital economy – as a connected social machine

The emerging categories represent a decomposition of the digital economy into: domain communities, digital processes, digital societies, and social platforms. The digital economy connected to physical and human networks can operate as systems of systems and can act as mechanisms for real-time feedback distribution directly from users and markets. The inter-relationships between the elements in Table 1 are crucial for defining a security framework for the digital economy. The development of the Internet of People and Internet of Services requires a deeper understanding of the relationship between the IoT and the digital economy.

Furthermore, Table 2 shows that the next level of technological capabilities in the digital economy is related to the integration of IoT and cyber physical capabilities into the industrial value chains. IoT uses principles of integrating network intelligence, providing convergence, orchestration and visibility across otherwise disparate systems. The integration of such capabilities into the digital economy requires operation and management of multiple CPS-related elements, such as IoT, the Internet of People and Internet of Services operating as Social Machines. The categories from Table 1 are correlated in a hierarchical framework in Table 2, to correspond with the new understanding of the digital economy.

Glossary of acronyms 3: Grouping of concepts for individual levels of the 5C architecture	
Self-maintaining connection	
Software assurance and application security	
Big data platform	BDP
Mobile CPS	mCPS
Required:	
Condition based monitoring	CBM
Self-aware conversion	
Life cycle and anti-counterfeit	
Task specific human machine interfaces	HMI
Self-aware machines and components	MaC
Anti-malicious and anti-tamper	
Loosely time-triggered architectures	LTTA
Structure dynamics control	SDC
Required:	
Prognostics and health management	PHM
Cyber self-compare	
Electronic and physical security	
Real-time data acquisition and storage solutions	RTD
Fleet of machines	FoM
Adaptive analysis	AA
Peer-to-peer monitoring	PtPM
Required:	
Cyber physical systems	CPS

Self-predicting cognition	
Diminishing manufacturing sources, material shortages and supply chain risk management	
Prioritising and optimising decisions	POD
Self- optimising production systems	SOPS
Information assurance and data security	
Autonomous cognitive decisions	ACD
Machine learning algorithms	MLA
High performance computing for data analysis	HPC
Information sharing and reporting	ISR
Required:	
Decision support system	DSS
Self-organising and self-configuring	
Track and trace	
Supervisory control of actions to avoid or grant access	CoA
Forensics, prognostics, and recovery plans	
Key performance indicators	KPI
Asset management and access control	
Cyber-Physical Production Systems	CPPS
Required:	
Resilient control system	RCS

Table 2: Hierarchical framework of the digital economy to correspond with the concept of a social machine

4.1 Proposed architecture for the digital economy as a social machine

The architecture in Table 2 includes: (1) self-maintaining machine connection for acquiring data and selecting sensors; (2) self-awareness algorithms for conversion of data into information; (3) connecting machines to create self-comparing cyber network that can predict future machine behaviour; (4) capacity to generate cognitive knowledge of the system to self-predict and self-optimise, before transferring knowledge to the user; (5) configuration feedback and supervisory control from cyber space to physical space, allowing machines to self-configure, self-organise and be self-adaptive.

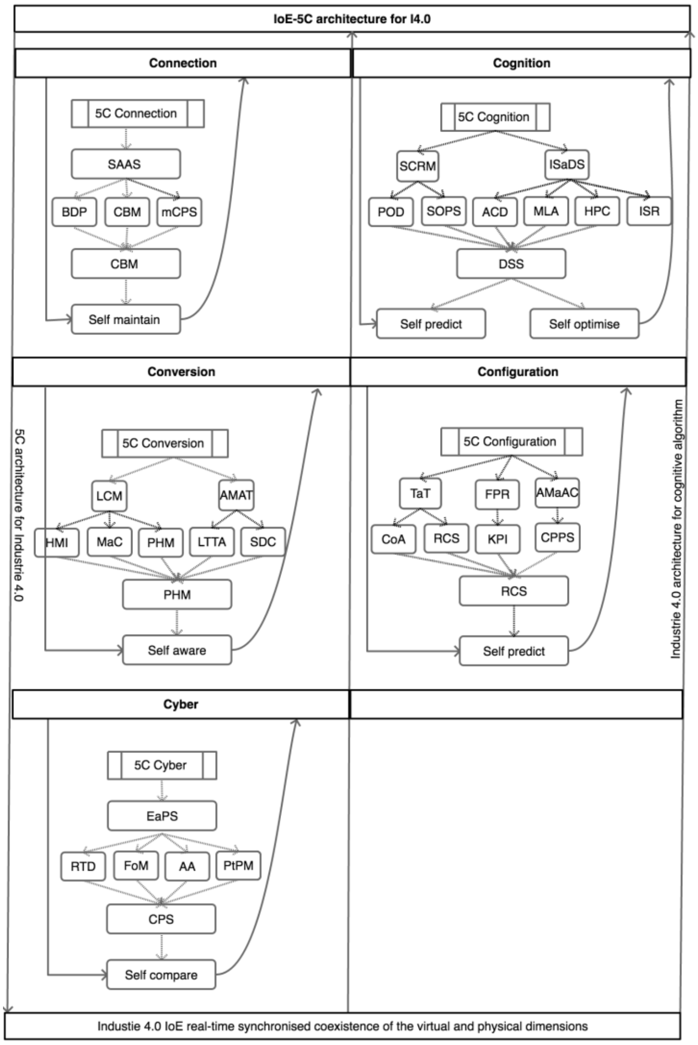

Figure 2: Hierarchical cascading model – digital economy operating as a social machine

The emerging hierarchical cascading model in Figure 2 visualises their relationships in the digital economy. Figure 2 presents the way the digital economy can connect and exchange information through cyber network. The described digital economy concept represents cognitive architecture. The emergence of cyber cognition confirms that the proposed architecture for the digital economy operates in a similar method with social networks.

5 Discussion

The architectural model presented in this paper is designed to support the building of new type of digital economy, based on the existing frameworks and practical initiatives. The architecture model would also benefit practitioners who aim to evolve their production models in the digital economy space.

5.1 Validation of the model

Table 3 summarises the main elements of this study and indicates where individual aspects of the presented architecture are being implemented. However, testing this research requires development of testbeds to validate the proposed solutions. In the current scenario where testbeds have limited deployment capabilities for complex computation, the model design should be further validated through case studies.

5.2 *Limitations and areas for further research*

The architecture model requires further validation and delimiting through application to real world case studies. The process of implementing the future developments in the digital economy is an evolutionary process, and as such, it would require flexibility in adapting the proposed framework to synchronise changes in the system complexities.

6 Conclusions

The contribution of this paper is two-fold. Firstly, it advances current knowledge by presenting an up-to-date overview of existing and emerging advancements in the IoT field in relation to the digital economy. The paper combines and incorporate existing understanding into new reference architecture for the digital economy. Secondly, the paper captures some of the best practices in industry on the development of a reference architecture for the digital economy using a step-by-step process analysis. This analysis includes reflection on how automation and AI could lower the cyber risk from the future developments in the digital economy.

Author Contributions: Conceptualization, Petar Radanliev, David De Roure, Jason R.C. Nurse, Razvan Nicolescu, Michael Huth, Stacy Cannady and Rafael Mantilla Montalvo; Data curation, Petar Radanliev; Formal analysis, Petar Radanliev; Funding acquisition, Petar Radanliev; Investigation, Petar Radanliev and David De Roure; Methodology, Petar Radanliev, Razvan Nicolescu, Stacy Cannady and Rafael Mantilla Montalvo; Project administration, Petar Radanliev; Resources, Petar Radanliev; Supervision, David De Roure, Jason R.C. Nurse, Michael Huth, Stacy Cannady and Rafael Mantilla Montalvo; Validation, Petar Radanliev; Visualization, Petar Radanliev and Razvan Nicolescu; Writing – original draft, Petar Radanliev; Writing – review & editing, Petar Radanliev.

Funding: This research was funded by the UK EPSRC with project [grant number EP/N02334X/1 and EP/N023013/1] and by the Cisco Research Centre [grant number 2017-169701 (3696)].

Acknowledgments: Sincere gratitude to the Fulbright Commission for supporting this project with the Fulbright Visiting Fellowship at MIT and the University of North Carolina.

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

References:

[1] R. Nicolescu, M. Huth, P. Radanliev, and D. De Roure, "State of The Art in IoT - Beyond Economic Value," London, 2018.

[2] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, and P. Burnap, "Supply Chain Design for the Industrial Internet of Things," Oxford, 2019.

[3] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, and P. Burnap, "The Industrial Internet-of-Things in the Industry 4.0 supply chains of small and medium sized enterprises," Oxford, 2019.

[4] P. Radanliev, "Green-field Architecture for Sustainable Supply Chain Strategy Formulation," *Int. J. Supply Chain Manag.*, vol. 4, no. 2, pp. 62–67, Jun. 2015.

[5] P. Radanliev, "Architectures for Green-Field Supply Chain Integration," *J. Supply Chain Oper. Manag.*, vol. 13, no. 2, Sep. 2015.

[6] P. Radanliev and D. C. De Roure, "Decision support system for visualising cyber risk from IoT technologies in supply chains," Oxford, 2019.

[7] P. Radanliev, D. C. De Roure, J. R. C. Nurse, P. Burnap, E. Anthi, U. Ani, O. Santos, and R. M. Montalvo, "Definition of Cyber Strategy Transformation Roadmap for Standardisation of IoT Risk Impact Assessment with a Goal-Oriented Approach and the Internet of Things Micro Mart," Oxford, 2019.

[8] P. Radanliev, "A conceptual framework for supply chain systems architecture and integration design based on practice and theory in the North Wales slate mining industry," British Library, 2014.

[9] P. Radanliev, H. Rowlands, and A. Thomas, "Supply Chain Paradox: Green-field Architecture for

Sustainable Strategy Formulation," in *Cardiff: Sustainable Design and Manufacturing 2014, Part 2, International Conference*, 2014, pp. 839–850.

[10] P. Radanliev, "Supply Chain Systems Architecture and Engineering Design: Green-field Supply Chain Integration," *Oper. Supply Chain Manag. An Int. J.*, vol. 9, no. 1, 2016.

[11] P. Radanliev, "Engineering Design Methodology for Green-Field Supply Chain Architectures Taxonomic Scheme," *J. Oper. Supply Chain Manag.*, vol. 8, no. 2, pp. 52–66, Dec. 2015.

[12] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, "Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, vol. 2018, no. CP740, p. 3 (9 pp.)-3 (9 pp.).

[13] P. Radanliev, D. De Roure, R. Nicolescu, M. Huth, R. M. Montalvo, S. Cannady, and P. Burnap, "Future developments in cyber risk assessment for the internet of things," *Comput. Ind.*, vol. 102, pp. 14–22, Nov. 2018.

[14] R. Nicolescu, M. Huth, P. Radanliev, and D. De Roure, "Mapping the values of IoT," *J. Inf. Technol.*, pp. 1–16, Mar. 2018.

[15] J. Nurse, S. Creese, and D. De Roure, "Security Risk Assessment in Internet of Things Systems," *IT Prof.*, vol. 19, no. 5, pp. 20–26, 2017.

[16] J. R. C. Nurse, P. Radanliev, S. Creese, and D. De Roure, "Realities of Risk: 'If you can't understand it, you can't properly assess it!': The reality of assessing security risks in Internet of Things systems," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1–9.

[17] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, P. Burnap, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, and Stacy Cannady, "Design principles for cyber risk impact assessment from Internet of Things (IoT)," Oxford, 2018.

[18] L. Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, H. Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, D. Cooper, R., Coulton, P., Craggs, B.,Davies, N., De Roure, B. Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, A. Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, R. Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, T. Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., and P. S. R.J., Westbury, "Internet of Things realising the potential of a trusted smart world," London, 2018.

[19] P. Radanliev, C. D. De Roure, .R.C. Nurse, R. Nicolescu, M. Huth, C. Cannady, R. M. Montalvo, D. De Roure, J. R. C. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, "Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-things in Industry 4.0," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, vol. 2018, no. CP740, p. 41 (6 pp.)-41 (6 pp.).

[20] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, and P. Burnap, "Cyber risk impact assessment for the Internet of Things (IoT)," *Work. Pap.*, 2019.

[21] P. Radanliev, D. C. De Roure, J. R. C. Nurse, P. Burnap, E. Anthi, U. Ani, L. Maddox, O. Santos, and R. M. Montalvo, "Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment," Preprints, Oxford, Mar. 2018.

[22] P. Radanliev, D. C. De Roure, J. R. C. Nurse, P. Burnap, E. Anthi, U. Ani, L. Maddox, O. Santos, and R. M. Montalvo, "Cyber risk from IoT technologies in the supply chain – discussion on supply chains decision support system for the digital economy," Oxford, 2018.

[23] P. Radanliev, D. De Roure, J. R. C. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, "New

developments in Cyber Physical Systems, the Internet of Things and the Digital Economy – discussion on future developments in the digital economy," Oxford, 2018.

[24] P. Radanliev, D. De Roure, J. R. C. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, "Cyber risk impact assessment – discussion on assessing the risk from the IoT to the digital economy," Oxford, 2018.

[25] K. Ruan, "Introducing cybernomics: A unifying economic framework for measuring cyber risk," *Comput. Secur.*, vol. 65, pp. 77–89, 2017.

[26] J. Lee, B. Bagheri, and H.-A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," 2015.

[27] P. Radanliev, D. De Roure, R. Nicolescu, and M. Huth, "A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0," Oxford, 2019.