 doi:10.20944/preprints201903.0123.v1

Engineering Sciences Department
University of Oxford

SUPPLY CHAIN DESIGN FOR THE INDUSTRIAL INTERNET OF THINGS AND THE INDUSTRY 4.0

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

Petar Radanliev[1], David C. De Roure[1]; Jason R.C. Nurse[2]; Rafael Mantilla Montalvo[3]; Peter Burnap[4]

[1]Oxford e-Research Centre, 7 Keble Road, Engineering Sciences Department, University of Oxford, OX1 3QG, UK; [2]School of Computing, University of Kent, UK, [3]Cisco Research Centre, Research Triangle Park, USA; [4]School of Computer Science and Informatics, Cardiff University

Abstract: Digital technologies have changed the way supply chain operations are structured. In this article, we develop design principles to show determining factors for an Internet-of-Things approach within Supply Chain Management. From the design principles, the article derives a new model for the Industrial Internet of Things supply chains. The focus is on Small and Medium Enterprises (SMEs). This research design results in a new process of compounding knowledge from existing supply chain models and adapting the cumulative findings to the concept of supply chains in the Industrial Internet of Things. The paper outlines the design principles for developing cognition in the process of integrating SME's digital supply chains in the Industrial Internet of Things (IIoT) and the Industry 4.0 (I4.0).

Keywords: *Industry 4.0; Supply Chain Design; Transformational Design Roadmap; IIoT Supply Chain Model; Decision Support for Information Management*

 doi:10.20944/preprints201903.0123.v1

1 Introduction

The motivation for this article comes from the increased sense that digital technologies are changing how supply chain operations are structured [1]–[4]. A supply chain is a system for moving products from supplier to customer [5]–[8]. Supply chain operational changes from digital technologies would specifically affect the small and medium sized companies (SMEs) because they lack the expertise, know-how, experiences and technological recourses of large enterprises. SME's in this article refers to enterprises with less than 250 employees, turnover of less than £25m and gross assets of less than £12.5m. We argue that a model for businesses and supply chain strategies is needed for the SME's to adapt to the technologically changing environment. Literature confirms that relying on government support is not sufficient. This is because the business environments with highest cyber ranking [9], should have the strongest business impact [10]. However, these business environments drop much lower in the industry application of digital infrastructure [9]. The issues could be caused by the barriers imposed to adoption of smart manufacturing technologies, e.g. cost of computing power, cost of implementation or analysis software [11]. Investment in technology infrastructure could improve the business performance [11], however, some SME's lack even the basic digital capabilities [12]. This points to the need to develop the design principles for the integration of the Internet-of-Things and Industry 4.0.

1.1 The methodology

Methodologically, the article draws on a number of different sources and research methods, including a taxonomic review as a discourse of literature [13], case study research [14] including open and categorical coding, with discourse analysis and grounded theory [4], [15]. The data and the findings are synthesised using the grounded theory approach of categorising the emerging concepts [16]. The case study research was performed on five I4.0 national initiatives and their technological trends in relation to IIoT product and services for a diverse set of industries. The initial set contained 12 different I4.0 national initiatives and their technological trends. These were selected through convenience sampling, which is a type of non-probability sampling that involved the sample set being drawn from the national initiatives and their technological trends that were convenient to access. Only five of the initial selection of I4.0 national initiatives and their technological trends are analysed in more detail. These were chosen based on testing the content of the initial set, where it was discovered that the remaining seven initiatives do not discuss the I4.0 supply chains. This process corresponds with existing literature [17].

 doi:10.20944/preprints201903.0123.v1

2 Taxonomic review

The literature review covers a vast area of internet-of-things, cyber physical systems, industry 4.0, cyber security, and supply chain topics, e.g. digitisation, automation and autonomy. The literature review applies a taxonomic approach and follows the process of synthesising the most prominent categories, emerging from the reviewed literature. This follows the grounded theory approach of categorising emerging concepts [16]. The emerging categories from the review are classified with open and categorical coding [18] in the theory development chapter.

2.1 How SME's can integrate modern technological concepts into their supply chain management – technical challenges

The technical challenges for SME's integrating modern technological concepts, such as the I4.0 mostly evolve around the design challenges and the potential economic impact (loss) from cyber-attacks [19]–[27]. The integration of such technologies in supply chains creates cyber security risk, for example from integrating less secured systems [28]. To reduce these costs and cyber risk, the SME's need to integrate IIoT processes and services [29], [30] in the industrial value chain [31]–[33], for value creation and value capture [34], through machine decision making [35], [36] connected to the Internet of Services [37], [38]. In addition, access control is required for granting or denying requests for information and processing services [35], [39], [40]. Large enterprises have the recourses to control the entire supply chain [5]–[8], [41], while SME's frequently have to integrate their supply chain operations [42]–[45]. Integrating multiple SME's in the supply chain requires higher visibility and coordination between participants [21], [25], [27]. Hence, these recommendations are aimed at enabling SME's to visualise the design principles.

3 Case study of five leading I4.0 initiatives and their technological trends

The gaps and key factors in current technological trends for I4.0 supply chain design integrating IIoT principles were derived from the taxonomic review [1], [3], [27], [41], [42], [44]–[47], [19]–[26]. These are analysed through a case study of I4.0 frameworks in the current section. We have chosen to use a case study research-based methodology because it is recommended in recent literature for addressing the gaps in knowledge and for advancing the methodological rigour; this is done specifically by studying platforms on different architectural levels and in different industry settings [48]. The list of 15 initiatives reviewed included:

 doi:10.20944/preprints201903.0123.v1

I4.0 technological trends - national initiatives/frameworks
Germany - Industrie 4.0 [49].
USA - (1) Industrial Internet Consortium (IIC, 2017); (2) Advanced Manufacturing Partnership [50].
UK – (1) Catapults [51]; (2) UK Digital Strategy (DCMS, 2017); (2) Made Smarter review 2017 [52].
Japan - (1) Industrial Value Chain Initiative (IVI, 2017); (2) New Robot Strategy (NRS) [53] and RRI (METIJ, 2015).
France - New France Industrial (NFI) – also known as: la Nouvelle France Industrielle or Industry of the Future [55]
Nederland - Smart Industry; or Factories of the Future 4.0 [56].
Belgium - Made Different [57].
Spain - Industrie Conectada 4.0 [58].
Italy - Fabbrica Intelligente [59].
China - Made in China 2025 [60].
G20 - New Industrial Revolution (NIR) [61].
Russia - National Technology Initiative (NTI) (ASI, 2016).

Table 1: I4.0 technological trends, national initiatives and frameworks reviewed

The initiatives and their technological trends reviewed, embed the I4.0 and present a quick overview of the current state of the I4.0 supply chain adoption. The case study starts with the Industrial Internet Consortium [62], as the leading and most recent initiative, and follows with a case study of additional four I4.0 world leading initiatives.

These initiatives and their technological trends are applicable to SME's and to large enterprises. To identify the most prominent categories that apply to SME's supply chains, the comparative analysis applied the grounded theory approach to study and analyse the emerging trends and to organise into related categories and sub-categories. Through comparative analysis, a number of shortcomings in individual initiatives are identified. The main shortcoming identified was that the national strategies propose very different approaches - as seen in Table 2.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2019 doi:10.20944/preprints201903.0123.v1

	Design principles for SME's supply chains in I4.0			
I4.0 technological trends	Cloud integration of CPS and IIoT in I4.0	Real-time CPS and IIoT in I4.0	Autonomous cognitive decisions for CPS and IIoT in I4.0	Recovery plans for CPS and IIoT in I4.0
IIC, 2016	1. Cloud-computing platforms.	1. Adapt businesses and operational models in real time; 2. Customized product offers and marketing in real time.	1. Fully connected and automated production line; 2. Support highly automated and human operated environments.	Gap - disaster recovery mentioned, but not incorporated.
DCMS, 2016	1. Cloud technology skills; 2. Cloud computing technologies; 3. Cloud data centres; 4. Cloud-based software; 5. Cloud-based computing; 6. Cloud guidance.	1. Digital real-time and interoperable records; 2. Platform for real-time information.	1. UK Robotics and Autonomous Systems; 2. Support for robotics and artificial intelligence; 3. Encourage automation of industrial processes; 4. Active Cyber Defence.	x
IVI, 2017	1. Cloud enabled monitoring; 2. Integration framework in cloud computing.	x	1. Factory Automation Suppliers and IT vendors; 2. Utilisation of Robot Program Assets by CPS.s	x
Industrie 4.0	1. CPS automated systems; 2. Automated conservation of resources.	1. Cloud computing; 2. Cloud-based security networks.	1. Automated production; 2. Automated conservation of recourses.	x
NTI, 2015	Gap	x	1. Artificial intelligence and control systems	x

Table 2: Outline of design principles for SME's supply chains in I4.0 - emerging from the case study

Following the grounded theory approach [16], the main categories of each individual initiative are separated into subcategories in Table 2 according to their specific design principles. .

3.1 Design principles for I4.0 supply chains

We place an emphasis on a cognitive I4.0 model. Cognitive I4.0 model refers to the trend of automation, introduced by computing devices that are reasoning and making supply chain decisions for humans. The emerging applications and technologies are presented in the form of a grouping diagram (Figure 1) to visualise the required concepts for the integration of SME's supply chains in I4.0. The grouping of concepts starts with the most prominent categories emerging from the taxonomy of literature: (1) self-maintaining machine connection for acquiring data and selecting sensors; (2) self-awareness algorithms for conversion of data into information [63]–[65]; (3) connecting machines to create self-comparing cyber network that can predict future machine behaviour [63]; (4) generates cognitive knowledge of the system to self-predict and self-optimise, before transferring knowledge to

 doi:10.20944/preprints201903.0123.v1

the user [31]; (5) configuration feedback and supervisory control from cyber space to physical space, allowing machines to self-configure, self-organise and be self-adaptive [66].

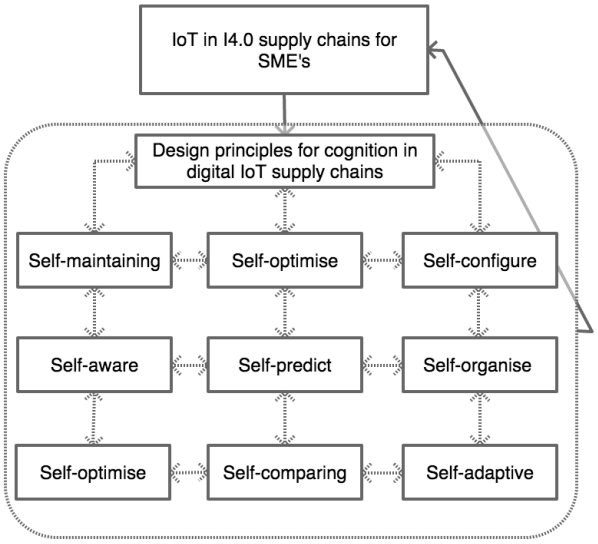

Figure 1: Design principles for cognition in digital IIoT supply chains

The described principles represent the beginning of a cognitive architecture for I4.0 supply chains. Such cognitive architecture allows for learning algorithms and technologies to be changed quickly and re-used on different platforms [31], [67], for creating multi-vendor production systems [65] which is necessary for the I4.0 supply chains. A cognitive production systems would provide real-time synchronised coexistence of the virtual and physical dimensions [38].

3.2 Discussion and main findings

The study applies taxonomic review and case study research to derive with the design principles for a theoretical model that enables the process of integrating SME's business and supply chains in the I4.0 network. The model captures the best practices in industry and defines the differences and similarities between I4.0 technological trends. Major projects on I4.0 are reviewed to present the landscape for cutting edge developments in IIoT, offering us a comprehensive picture of the current state of supply chain adoption.

4 Conclusion

The literature review discovered a lack of design clarification for the I4.0 supply chains. The literature review also discovered that adaptation of IIoT technologies, depends on the SME's cyber recourses. This specifically concerns SME's as they do not have the same supply chain recourses as large enterprises. The new design principles enable SME's to visualise the required cyber resources and the integration process for IIoT technologies. The case study research combined with the grounded theory

 doi:10.20944/preprints201903.0123.v1

methodology, advanced the design principles into a transformational roadmap. The transformational roadmap defined the integration process of IIoT technologies and consolidated the cyber themes of the future makeup of I4.0 supply chains. The grounded theory methodology was applied to build a new theoretical model from the compositions in the design process and the transformational roadmap. The theoretical model can also be applied by SME's already operating in the I4.0 to visualise and assess their exposure to cyber risk and to design cyber recovery. The theoretical model in this study proposes a decomposed operational system with concrete and workable action plans, that would transition the economic and social systems towards new cyber capabilities. Visualisation and decomposition of the required cyber capabilities and cyber recovery planning is surprisingly not covered in existing models.

4.1 Limitation of the study

This study focused on the integration of SME's supply chains in I4.0. While the findings may also be suited to large enterprises, the aim of this research was to develop a model for SME's with limited technologies and expertise. The technologies analysed, bring diverse set of cyber risks, which until present are not quantified. In further studies, the supply chain accumulated cyber risk needs to be quantified and this should also be investigated for larger enterprises.

5 References

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

[2] 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.

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

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] Allen and Hamilton, "Cyber Power Index: Findings and Methodology," McLean, Virginia, 2014.

[10] P. Marwedel and M. Engel, "Cyber-Physical Systems: Opportunities, Challenges and (Some) Solutions," Springer International Publishing, 2016, pp. 1–30.

[11] G. Anderson, "The Economic Impact of Technology Infrastructure for Smart Manufacturing,"

NIST Econ. Anal. Briefs, vol. 4, 2016.

[12] G. Baker, S. Lomax, P. Braidford, G. Allinson, and M. Houston, "Digital Capabilities in SMEs: Evidence Review and Re-survey of 2014 Small Business Survey respondents," 2015.

[13] B. Paltridge, "Peer Review in Academic Settings," in *The Discourse of Peer Review*, London: Palgrave Macmillan UK, 2017, pp. 1–29.

[14] J. Blatter and M. Haverland, *Designing Case Studies*. London: Palgrave Macmillan UK, 2012.

[15] 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.

[16] B. G. Glaser and A. L. Strauss, *The discovery of grounded theory : strategies for qualitative research*. Abingdon, Oxford: Routledge, 1967.

[17] M. Q. Patton and M. Q. Patton, *Qualitative research and evaluation methods*. Sage Publications, 2002.

[18] C. Goulding, *Grounded theory : a practical guide for management, business and market researchers*. SAGE, 2002.

[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 - 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. 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.).

[21] 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," University of Oxford, 2019.

[22] 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.

[23] 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)," University of Oxford, 2019.

[24] 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.

[25] 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, 201903.0080.v1, Mar. 2019.

[26] 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 – future developments in the Industrial Internet of Things and Industry 4.0," University of Oxford, 2019.

[27] P. Radanliev, D. De Roure, J. R. C. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, "Cyber risk impact assessment – assessing the risk from the IoT to the digital economy," University of Oxford, 2019.

[28] K. Carruthers, "Internet of Things and Beyond: Cyber-Physical Systems - IEEE Internet of Things," *IEEE Internet of Things*, Newsletter, 2014, 2016.

[29] T. Stock and G. Seliger, "Opportunities of Sustainable Manufacturing in Industry 4.0," *Procedia CIRP*, vol. 40, pp. 536–541, 2016.

[30] F. Hussain, "Internet of Everything," in *Internet of Things: Building Blocks and Business Models: SpringerBriefs in Electrical and Computer Engineering*, Springer International Publishing, 2017, pp. 1–11.

[31] M. Brettel, F. G. Fischer, D. Bendig, A. R. Weber, and B. Wolff, "Enablers for Self-optimizing

 doi:10.20944/preprints201903.0123.v1

Production Systems in the Context of Industrie 4.0," *Procedia CIRP*, vol. 41, pp. 93–98, 2016.
[32] M. Hermann, T. Pentek, and B. Otto, "Design Principles for Industrie 4.0 Scenarios," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 3928–3937.
[33] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing Smart Factory of Industrie 4.0: An Outlook," *Int. J. Distrib. Sens. Networks*, vol. 12, no. 1, pp. 1–10, Jan. 2016.
[34] J. M. Müller, O. Buliga, and K.-I. Voigt, "Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0," *Technol. Forecast. Soc. Change*, Jan. 2018.
[35] P. C. Evans and M. Annunziata, "Industrial Internet: Pushing the Boundaries of Minds and Machines," General Electric, 2012.
[36] L. Wang, "Machine availability monitoring and machining process planning towards Cloud manufacturing," *CIRP J. Manuf. Sci. Technol.*, vol. 6, no. 4, pp. 263–273, Jan. 2013.
[37] W. Wahlster, J. Helbig, A. Hellinger, M. A. V. Stumpf, J. Blasco, H. Galloway, and H. Gestaltung, "Recommendations for implementing the strategic initiative INDUSTRIE 4.0," Federal Ministry of Educationand Research, 2013.
[38] S. I. Shafiq, C. Sanin, E. Szczerbicki, and C. Toro, "Virtual Engineering Object / Virtual Engineering Process: A specialized form of Cyber Physical System for Industrie 4.0," *Procedia Comput. Sci.*, vol. 60, pp. 1146–1155, 2015.
[39] D. DiMase, Z. A. Collier, K. Heffner, and I. Linkov, "Systems engineering framework for cyber physical security and resilience," *Environ. Syst. Decis.*, vol. 35, no. 2, pp. 291–300, 2015.
[40] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-Physical Systems: The Next Computing Revolution," in *Proceedings of the 47th Design Automation Conference on - DAC '10*, 2010, p. 731.
[41] 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 and the Industry 4.0," University of Oxford, 2019.
[42] 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," University of Oxford, 2019.
[43] P. Radanliev, D. De Roure, J. Nurse, P. Burnap, and R. Mantilla Montalvo, "Methodology for designing decision support supply chain systems for visualising and mitigating cyber risk from IoT technologies," University of Oxford, 2019.
[44] 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," University of Oxford, 2019.
[45] 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 – decision support system for the Industry 4.0," University of Oxford, 2019.
[46] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, and P. Burnap, "Standardisation of cyber risk impact assessment for the Internet of Things (IoT)," University of Oxford, 2019.
[47] P. Radanliev, D. De Roure, C. Maple, R. Nicolescu, J. Nurse, and U. Anie, "Cyber Risk in IoT Systems," University of Oxford, 2019.
[48] M. de Reuver, C. Sørensen, and R. C. Basole, "The digital platform: a research agenda," *J. Inf. Technol.*, pp. 1–12, Apr. 2017.
[49] GTAI, "Industrie 4.0 Smart Manufacturing for the Future," Berlin, 2014.
[50] AMP, "Advanced Manufacturing Partnership," 2013.
[51] P. John, "High Value Manufacturing Catapult," Solihull, 2017.
[52] Siemens, "Made Smarter review 2017," 2017.
[53] METI, "NRS, New Robot Strategy - Vision Strategy and Action Plan; Ministry of Economy Trade and Industry of Japan," 2015.
[54] METIJ, "RRI, Robot Revolution Initiative - Summary of Japan's Robot Strategy - It's vision, strategy and action plan; Ministry of Economy, Trade and Industry of Japan," 2015.
[55] NIF, "New Industrial France: Building France's industrial future - updated text from the 2013 version," Paris, 2016.
[56] T. Bouws, F. Kramer, P. Heemskerk, M. Van Os, T. Van Der Horst, S. Helmer, S. Huveneers, M. Butter, F. Van Der Zee, S. Van Oort, J. Ypma, G. Mulder, B. Kotterink, and M. De Heide,

 doi:10.20944/preprints201903.0123.v1

"Smart Industry: Dutch Industry Fit for the Future," Delft, 2015.

[57] Sirris and Agoria, "Made Different: Factory of the Future 4.0," 2017. [Online]. Available: http://www.madedifferent.be/en/what-factory-future-40. [Accessed: 09-May-2017].

[58] MEICA, "Industria Conectada 4.0: La transformación digital de la industria española Dossier de prensa; Ministry of Economy Industry and Competitiveness Accessibility," Madrid, 2015.

[59] MIUR, "Italian Technology Cluster: Intelligent Factories; Ministry of Education Universities and Research," *Cluster Tecnologico Nazionale Fabbrica Intelligente | Imprese, università, organismi di ricerca, associazioni e enti territoriali: insieme per la crescita del Manifatturiero*, 2014. [Online]. Available: http://www.fabbricaintelligente.it/en/. [Accessed: 09-May-2017].

[60] SCPRC, "Made in China 2025; The State Council People Republic of China," *www.english.gov.cn*, 2017. [Online]. Available: http://english.gov.cn/2016special/madeinchina2025/. [Accessed: 10-May-2017].

[61] G20, "G20 New Industrial Revolution Action Plan," 2016.

[62] IIC, "The Industrial Internet of Things, Volume B01: Business Strategy and Innovation Framework; Industrial Internet Consortium," 2016.

[63] J. Lee, H.-A. Kao, and S. Yang, "Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment," *Procedia CIRP*, vol. 16, pp. 3–8, 2014.

[64] C. Toro, I. Barandiaran, and J. Posada, "A Perspective on Knowledge Based and Intelligent Systems Implementation in Industrie 4.0," *Procedia Comput. Sci.*, vol. 60, pp. 362–370, 2015.

[65] S. Weyer, M. Schmitt, M. Ohmer, and D. Gorecky, "Towards Industry 4.0 - Standardization as the crucial challenge for highly modular, multi-vendor production systems," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 579–584, 2015.

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

[67] O. Niggemann, G. Biswas, J. S. Kinnebrew, H. Khorasgani, S. Volgmann, and A. Bunte, "Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control," in *International Workshop on the Principles of Diagnosis (DX)*, 2015, pp. 185–192.