doi:10.20944/preprints201903.0139.v1

A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0

Petar Radanliev[1], David De Roure[1], Razvan Nicolescu[2], Michael Huth[2]

[1]Oxford e-Research Centre, 7 Keble Rd, Oxford OX1 3QG

[2]Department of Computing, Imperial College London, Huxley Building, 180 Queen's Gate, London, SW7 2AZ

Abstract

There is an increased attention on propositions on models, infrastructures and frameworks of IoT in both business reports and technical papers. These reports and publications frequently represent a juxtaposition of other related systems and technologies (e.g. Industrial Internet of Things, Cyber Physical Systems, Industry 4.0 etc). At present, the literature is missing a design process for integrating these constantly evolving systems and technologies in a clear and understandable step by step model. This paper contributes with a new reference architecture model for the integration of these systems and technologies. The reference architecture model is based on grouping of future and present techniques and presenting the design process through a new hierarchical framework and a new cascading model. With the application of the grounded theory, the hierarchical framework and the cascading model detail a new process for creating a taxonomy of categories and grouping of concepts into integration design. The new design process is tested and versified with an empirical review of Industry 4.0 frameworks and results with a new 5 levels reference architecture step by step model for the integration of these related systems and technologies (Industrial Internet of Things, Cyber Physical Systems, and Industry 4.0). We review 118 academic and industry papers published between 2010 and 2019. Then, we report the results of a qualitative empirical study that correlates academic literature with 14 world leading Industry 4.0 frameworks and initiatives. We therefore propose an architectural model that offers a better understanding of the systems integration between the Industrial Internet of Things and Industry 4.0.

Keywords: Industrial Internet of Things; Cyber Physical Systems; Internet of Everything; Industry 4.0; Digital Industry; Digital Economy.

Funding sources: This work was supported 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)].

Declarations of interest: none

Acknowledgements: Sincere gratitude to the Fulbright Commission

1. Introduction

The evolution of the Industrial Internet of Things (IIoT) technology has become of considerable academic, government and industry interest in recent years. The IIoT can be explained as the use of internet of things technologies to improve manufacturing and industrial processes. The IIoT term is closely related to the term Industry 4.0 (I4.0), which 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 (Wahlster et al., 2013), the 'New Industrial France' (NIF, 2017), the 'Industrial Internet' (Evans and Annunziata, 2012), the 'Internet and the Advanced Manufacturing Partnership' (AMP, 2013) or The Fourth Industrial Revolution (Carruthers, 2016). This article discusses major initiatives in this space in relation to the integration of different developments of cyber physical systems in I4.0 to better understand cyber risks and economic models.

It has been argued that the spectacular advancements in Cyber Physical Systems (CPS) and Internet of Things (IoT) technology represent the foundation for the I4.0 (Wahlster et al., 2013) The IoT term originated in 1999 (Ashton, 2009) along with the first view of how an IoT-based environment might look like in the future (Gershenfeld, 1999). 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 (Tan, Goddard, and Pérez, 2008; Madakam, Ramaswamy, and Tripathi 2015). 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. CPSs thus link the physical and engineered systems, and bridge the cyber world with the physical world (Rajkumar et al., 2010; Wahlster et al., 2013; Carruthers, 2016).

In contrast, IoT theory emerges from computer science and internet technologies and focuses mainly on interconnectivity, interoperability and integration of physical components in the Internet. Integration work that would lead to developments such as IoT automation of CPS (Dworschak and Zaiser, 2014; Ringert, Rumpe, and Wortmann, 2015), real-time enabled CPS platforms (Tan, Goddard, and Pérez, 2008; Shi *et al.,* 2011; Kang and Kapitanova, 2012; Kumar *et al.,* 2012; Wahlster et al., 2013; Marwedel and Engel, 2016), and automated CPS to guide skilled workers in production environment, is anticipated with the full IoT market adoption over the next decade (Gubbi *et al.,* 2013).

In this context, we propose the term CPS-IoT to refer to the integration of cyber physical attributes into IIoT systems. This integration includes advances in real-time processing, sensing, and actuation between IIoT systems and physical domains and provides capabilities for system analysis of the cyber and physical structures involved. We therefore focus here on the emerging Internet of Everything (IoE), defined as the networked connection of people, processes, data, and things (Cisco, 2013). Therefore, IoE represents a more inclusive and encompassing concept that consolidates the cyber physical attributes of IIoT with the social aspects of the environment in which this technology is actually deployed, and reflects the future makeup of IIoT/I4.0. The term IoE in the context of this article is used to discuss effect from the evolving IoT services and social networks of I4.0.

The research reported here has two research objectives. Firstly, we present an up-to-date overview of existing and emerging IIoT advancements in the field of I4.0. This combines existing literature in order to derive common basic terminology and approaches and to incorporate existing standards into a new IIoT reference architecture for I4.0. Secondly, we capture the best practices in industry and provoke a debate among practitioners and academics by offering a new theoretical model regarding I4.0. We develop an I4.0 reference architecture to enable the visualisation of network cyber risk, the minimization of cyber risk, and the integration of IIoT in the I4.0. This reference architecture for I4.0 can serve as a best practice and inform initial steps taken by organisations in this space.

This article is structured as follows. Our methodology is described in Section 1.1. In Section 2, we discuss the economic impact of cyber risks associated with IIoT and CPS in general. Section 3 produces a taxonomy for management techniques and production economies for I4.0. Section 4 offers a vision for integrating IIoT in Industry 4.0. A Discussion section and a Conclusions section synthesise our findings and end the article.

1.1 Method

The methods applied in this study consist of systematic literature review, taxonomies derived from grounded theory and conceptual model development, followed by a qualitative empirical study that engages with a variety of secondary resources. Academic literature and practical studies are consulted intensively to discuss the IoT technologies and their relation to the I4.0. While the mainstream academic literature offers limited insights regarding existing and emerging IIoT developments, we use major projects on I4.0 to showcase recent developments in this field. Our rationale is that – as the landscape of IIoT 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, combined with the grounded theory approach (Glaser and Strauss, 1967) in order to construct a conceptual cascading model for the integration of IIoT in the I4.0. These models then inform a qualitative empirical study for the new I4.0 architectural reference model. The chosen method for conducting systematic literature review represented (1) searching established journal databases and updating the findings with cross checking with google scholar search engine; (2) creating a table of search terms and article inclusion criteria such as relevance, peer review, data of publication (less than 10 years), and design of studies; (3) we also considered ethical issues in relations to how the publications obtained data, was the data reported accurately, and was the identity of individuals protected.

2. Economic Impact of Cyber Risks associated with IIoT and I4.0

The exact economic impact of CPS infrastructure still remains to be determined (Leitão, Colombo and Karnouskos, 2016; Marwedel and Engel, 2016), although CPS systems will represent a large percentage of future ICT application in industry (Marwedel and Engel, 2016). This situation requires a new theoretical model that integrates the physical and cyber subsystems of CPS and IIoT (CPS-IIoT) and goes beyond the M2M applications. The new theoretical model needs to provide an overall understanding of the design, development, and evolution of CPS, and .needs to integrate theories of IIoT, control of physical systems, as well as their interaction with humans.

Such a theoretical model is especially needed for developing nations that lack an I4.0 strategy, but also for more developed countries – such as the UK and USA. The UK has been ranked as the overall global cyber superpower followed by the US (Allen Hamilton, 2013). It is also reported that the UK and US are strongly protected to withstand digital infrastructure cyber-attacks, which is crucial in developing a resilient digital economy (Marwedel and Engel, 2016). However, in the index quantifying industrial applications in digital infrastructure key sectors, the UK drops down to the 5th place and the US to the 3rd place. This seems to be partly due to the UK and US lagging behind other countries in terms of harnessing economic value from the I4.0 (Allen Hamilton, 2013). This could be caused by barriers imposed to the adoption of smart manufacturing technologies, especially in small or medium enterprises, e.g. significant cost of computing power and analysis software (Anderson, 2016, Nicolescu 2018a,b).

There is an enormous economic potential for hyper-connected economy as literature recognises that important future business opportunities lay in the networking potential of digital economy (Bauer, Hämmerle, Schlund and Vocke, 2015). The infrastructure for smart manufacturing technology could create large cost savings for manufacturers (Anderson, 2016) and enable faster development of economies of scale (Brettel et al., 2016). Industrial Internet, or 'Industry 4.0,' supports a finer granularity and control to meet individual customer requirements, creates value opportunities (Brettel et al., 2016; Hermann, Pentek, and Otto, 2016, Shafiq, Sanin, Szczerbicki, and Toro, 2015; Stock and Seliger, 2016; Wang et al., 2016), increases resource productivity, and provides flexibility in business processes (Hussain, 2017). The integration of cyber-physical capabilities into IIoT arguably requires a new process model for integrating physical and cyber subsystems – including an overall understanding of the design, development, and evolution of CPS and IIoT. Gaining such understanding may require consolidation of IIoT theories for control of physical systems and the interaction between humans and CPS (Marwedel and Engel, 2016).

On the other hand, the US National Institute of Standards and Technology (US NIST) deliberately stays away from formalising any process model in this space (NIST, 2016). Instead, their recent Framework for Cyber Physical Systems proposes sets of artefacts and activities that could be considered by organisations in the deployment of CPS. These proposals are the result of formal ontologies of digital artefacts and their interactions with the exterior world. The US NIST identifies three main views on CPS that encompass identified responsibilities in the systems engineering process: conceptualization, realization, and assurance. Each of these three views corresponds to particular fundamental processes in the life of CPS, respectively: (1) Models of CPS (design), (2) the CPS itself (implementation), and (3) CPS Assurance (validation). In particular, the tradeoffs between different instantiations of these processes as well as between critical aspects such as Security, Safety, Business, and Privacy need to be understood. In this context, Risk Engineering is proposed as an activity embedded in the design, development and lifecycle of the future CPS and IoT systems (Huth et. al., 2016). This vision assumes that cyber risk is just one particular instantiation of risk for a particular organization or product and therefore should be subject to the higher processes of compliance and regulation in each domain (Nurse 2017, 2018). Building on this work, the reference architecture presented in Figure 3 aims to help industrial and academic research with formalizing compositional ways to reason about cyber risks in an I4.0 context.

There is an inherent risk in integrating the physical with the cyber world. The Cyber risk environment is constantly changing (DiMase et al., 2015), and estimated loss of cybercrime varies greatly (Biener, Eling and Wirfs, 2014; DiMase et al., 2015; Shackelford, 2016). The real economic impact of cyber risk remains unknown (Shackelford, 2016), mainly due to lack of suitable data and lack of a universal, standardised impact assessment framework (Koch and Rodosek, 2016). To develop such a framework, accumulated risk needs to be quantified and shared across technology platforms (Ruan, 2017). This requires detailed a understanding of the I4.0 network and critical infrastructure cyber risk. In addition, new risk elements also need to be quantified, such as intellectual property of digital information (Koch and Rodosek, 2016) and the impact of media coverage (Biener, Eling and Wirfs, 2014).

The Cyber Value at Risk (CvaR) model (World Economic Forum, 2015; Delloite, 2016) represents an attempt to understand the economic impact of cyber risk for individual organisations (Koch and Rodosek, 2016). CVaR provides cyber risk measurement units (Ruan, 2017), value analysis methods related to the cost of different cyber-attacks type (Roumani et al., 2016), and proof of concept methods that are based on data assumptions (Koch and Rodosek, 2016). Given the lack of data needed to validate the CvaR model, these studies calculate the economic impact based on organisations' 'stand-alone' cyber risk and therefore ignore the correlation effect of sharing infrastructure and information and the probability of 'cascading impacts' (DiMase et al., 2015, Radanliev 2018a,b,c, 2019a-f) which represents a crucial element of I4.0. These limitations of the CvaR model are of great concern, e.g in sharing cyber risk in critical infrastructure (Zhu, Rieger, and Basar, 2011; Koch and Rodosek, 2016). Critical infrastructures are vital for strong digital economies, but issues of synchrony, components failures, and increasing complexity demand development and elaboration of new rigorous CPS methods (Rajkumar et al., 2010). In the absence of a common reference point of cyber risks, existing cyber risk assessment methodologies have led to inconsistencies in measuring risk (Ruan, 2017), which negatively affects the adaptation of I4.0. Assessment of IIoT cyber risk in I4.0 should be based on a reference architecture that enables visualising and assessing the cyber network risk, not only the stand-alone cyber risks of a sole company.

In early literature, existing financial models have been proposed to assess information security investment (Anderson and Moore, 2006; Gordon and Loeb, 2002; Mercuri, 2003; Rodewald, 2005). However, cyber risk covers more elements than information security financial cost, such as brand reputation or intellectual property (Ruan, 2017; Koch and Rodosek, 2016). In terms of modelled economic and financial impact of massive cyber-attacks, additional questions emerge in relation to the impact on public sector, rethinking of business processes, growth in liability risk, and mitigation options (Ruffle et al., 2014). Such economic evaluations trigger a debate between limited economic lifespans of digital assets (Ruan, 2017) and value in inheriting 'out of date' data (Tan, Goddard, and Pérez, 2008). In an I4.0 context, cyber risks are not simply associated with machines and products that store their knowledge and create a virtual living representation in the network (Drath and Horch, 2014) but also to the global flows and markets they are part of.

Our literature review concludes that existing production economics models don't anticipate risks in sharing infrastructure and the probability of cascading impacts. We address this by proposing a reference architecture and associated best practices for I4.0 – applicable to any I4.0 initiatives.

3. Taxonomy of management technologies and methodologies for the I4.0 production economy

This section defines 5C architecture and creates a taxonomy representing a list of focal points for visualising and focusing the IoE-5C direction I4.0. To define the contribution from this study, we first explain the existing 5C architecture in Figure 1.

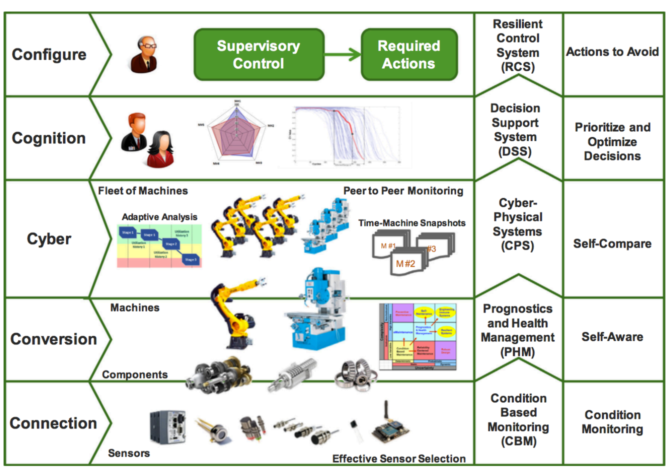

Figure 1: 5C architecture (Lee, Bagheri and Kao, 2015)

The aim of this study is to design a 5C architecture that can be adapted quickly (Niggemann et al., 2015; Brettel et al., 2016), to create multi-vendor and modular production systems (Weyer et al., 2015). Requiring multi-discipline testing and verification (Balaji et al., 2015), and understanding of system sociology (Dombrowski and Wagner, 2014), and should operate in a similar method with social networks (Bauer, Hämmerle, Schlund, and Vocke, 2015; Wan, Cai, and Zhou, 2015).

3.1 Cyber risk for integration of CPS-IIoT physical, information, and financial flows into I4.0

Industry 4.0 goes beyond machine to machine (M2M) CPS (Wan et al., 2013; Stojmenovic, 2014), and beyond the proposed 3 level CPS, which are: (1) services, (2) cloud, and (3) physical object layers (Drath and Horch, 2014). I4.0 is based on the 5C architecture - 5 level CPS (as seen in Figure 3, with intelligent manufacturing equipment (Lee, Bagheri, and Kao, 2015; Leitão, Colombo and Karnouskos, 2016; Marwedel and Engel, 2016; Shafiq, Sanin, Szczerbicki, and Toro, 2015; Toro, Barandiaran, and Posada, 2015).

The integration of artificial intelligence (AI), machine learning, the cloud, and IoT creates systems of machines capable of interacting with humans (Wan et al., 2013; Brettel et al., 2016; Carruthers, 2016; Marwedel and Engel, 2016). The application of behaviour economics into these systems of machines (Leonard, 2008) already enables market speculation on human behaviour (Rutter, 2015) and even neuromarketing (Lewis and Brigder, 2004) to determine consumer purchasing behaviour. We can expect to see autonomous machines adopting the use of these methods in order to predetermine human behaviour (Carruthers, 2016). Technologies that would enable the integration of IIoT and CPS include software defined networks (Kirkpatrick, 2013) and software defined storage (Ouyang et al., 2014). The foundations of IIoT and CPS industrial integration are built upon: protocols and enterprise grade cloud hosting (Carruthers, 2016); AI, machine learning, and data analytics (Wan et al., 2013; Kambatla et al., 2014; Pan et al., 2015; Shafiq, Sanin, Szczerbicki, and Toro, 2015); and mesh networks and peer-to-peer connectivity (Wark et al., 2007). IIoT transforms the embedded control of CPS, creating security and risk management vulnerabilities from integrating less secured systems, triggering questions regarding risk management and liability for breaches and damages (Carruthers, 2016). Many other technical challenges can be foreseen in the CPS in economically vital domains – especially in the design, construction and verification of CPS.

3.2 CPS in I4.0 - key management technologies

The academic literature we analysed outlines the evolution of CPS into the more inclusive and encompassing IoE. IoE brings together people, process, data, and things – making networked connections and transactions more valuable to individuals, organizations, and things (Cisco, 2013). 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 IIoT and industrial digitisation to gain competitiveness; (d) and utilization of Big Data to improve the efficiency of production and services. These requirements are analysed and categorised in Table 1 as: domain communities, processes, societies, and platforms.

3.3 IoE-CPS for I4.0 - the changing roles of innovation, production, logistics, and the service processes

The changing roles of innovation, production, logistics, and the service processes in IoE-CPS-I4.0 integration requires: (a) domain communities; (b) internet-based system and service platforms; (c) business processes and services; (d) dynamic intelligent swamps of physical and human networks.

Domain communities include: Agent-oriented Architecture (Ribeiro, Barata, and Ferreira, 2010), Object-oriented Architecture (Thramboulidis, 2015), Cloud optimised Virtual Object Architecture (Giordano, Spezzano, and Vinci, 2016), supported with Virtual Engineering Objects and Virtual Engineering Processes (Shafiq, Sanin, Szczerbicki, and Toro, 2015) with Internet Protocol version 6 (IPv6) connected devices and networks to the IoT (Wahlster et al., 2013);

Internet-based system and service platforms (La and Kim, 2010; Wahlster et al., 2013; Wan, Cai, and Zhou, 2015; Weyer et al., 2015) are used to model CPS through the Web of Things (Dillon et al., 2011). In particular, cyber risk in I4.0 requires compiling of data, processes, devices and systems for advanced analytics (Evans and Annunziata, 2012; Shafiq, Sanin, Szczerbicki, and Toro, 2015) and connection to model-driven (robot-in-the-loop) manufacturing systems (Jensen, Chang, and Lee, 2011; Shi et al., 2011; Wang et al., 2014). Internet-based system and service platforms are also used to promote model-based development platforms, such as behaviour modelling of robotic systems (Stojmenovic, 2014) or Automata (Ringert, Rumpe, and Wortmann, 2015). Internet-based systems and service platforms can also enable the development of social manufacturing (Bauer, Hämmerle, Schlund, and Vocke, 2015; Wan, Cai, and Zhou, 2015), nterconnect with the Internet of People (Wahlster et al., 2013) and create CPS collaborative communities (Lee, Kao, and Yang, 2014);

Business processes and services can be interconnected through IoT systems (Stock and Seliger, 2016; Hussain, 2017) into industrial value chains (Brettel et al., 2016; Hermann, Pentek, and Otto, 2016; Shafiq, Sanin, Szczerbicki, and Toro, 2015; Wang et al., 2016). Business processes and services can integrate machine information into decision making (Evans and Annunziata, 2012; Wan et al., 2013; Toro, Barandiaran, and Posada, 2015) and be connected to the Internet of Services (Wahlster et al., 2013; Shafiq, Sanin, Szczerbicki, and Toro, 2015) for service oriented architecture (La and Kim, 2010; Wang, Törngren, and Onori, 2015; Weyer et al., 2015) and Cloud distributed process planning manufacturing (Wang, 2013; Wan, Cai, and Zhou, 2015). Business processes and services can also promote knowledge development of business areas and applications (Faller and Feldmüller, 2015; Toro, Barandiaran, and Posada, 2015; Hussain, 2017).

Dynamic intelligent swamps (Giordano, Spezzano, and Vinci, 2016) of modules connected to physical and human networks (Evans and Annunziata, 2012; Marwedel and Engel, 2016), can operate as systems of systems (Wang, Törngren, and Onori, 2015, Leitão; Colombo and Karnouskos, 2016) and can act as mechanisms for real-time distribution (Tan, Goddard, and Pérez, 2008; Shi et al., 2011; Kang and Kapitanova, 2012) and feedback (Marwedel and Engel, 2016) directly from users and markets.

The key contributors to the integration of cyber physical capabilities into an IoE environment (CPS-IoE) are presented in Table 1. The relationships of these elements to CPS can be grouped into the following categories: CPS-IoE communities, CPS-IoE processes, CPS-IoE societies and CPS-IoE platforms. These contributors and the synergies between them lead to an integrated cyber risk aware process for I4.0 that is discussed further in the section.

Glossary of acronyms 1: Categories of key elements to integrate CPS in IoE	
CPS-IoE 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
CPS-IoE processes	
Connected devices and networks	CDN
Compiling for advanced analytics	CfAA
Business processes and services	BPS
Cloud distributed process planning	DPP

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

Physical and human networks	PHN
CPS-IoE societies	
Internet of Things	IoT
Web of Things	WoT
Social manufacturing	SM
Internet of People	IoP
Internet of Services	IoS
Systems of systems	SoS
CPS-IoE 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: Categories of key contributors to integrate CPS in IoE - derived from the taxonomy of literature

From reading the categorisation in Table 1, one point appears as an error in the categorisation. That is the Internet Protocol v6 is categorised as a platform, while from an engineering perspective IPv6 is a networking protocol. There are multiple categorisations that appear as errors of this type. The explanation for this categorisation is that to reduce the categories and themes, the grounded theory approach used the Pugh controlled convergence and in the process, themes are associated with the 'best fit' categories. The rationale for this categorisation is as follows. Protocol (e.g. the Internet Protocol v6) is the official procedure or system of rules governing the communication or activities of programs and/or industries. Platform on the other hand refers to the technologies that are used as a base upon which other applications, processes or technologies are developed. A CPS in the context of this categorisation is a platform, while the languages it uses to communicate (e.g. IPv6) with software are the protocol. Further clarification as why such categorisations have been made by applying the Pugh controlled convergence to reduce the number of categories is that we can consider a platform as a software, while protocol is more like a theory, or theoretical model which a platform can be based on. The outlined categorisation process (Table 1 and Table 2) has triggered a long debate among the Pugh controlled convergence participants. Finally, in the interest of keeping the categories and themes to a level that can easily be understood, the presented categorisations have been accepted for the abbreviated taxonomy in Table 2.

CPS - IoE

CPS-IoE communities	CPS-IoE processes	CPS-IoE societies	CPS-IoE platforms
5C: AoA, OoA, VOA, VEO, VEP	CDN	IoT	IPv6
MDMS	CfAA	WoT, SM, IoP	ISP, MBDP
SoA	BPS, DPP	IoS	KDoA
DIS	PHN	SoS	RtD

Table 2: Taxonomy of abbreviations from categories derived in the review of literature shown in Table 1

The taxonomy of abbreviations in Table 2 was derived from the taxonomy of literature in Table 1, which categorises the emerging concepts into integration structure. The taxonomic integration structure relates the industrial CPS with IoE, bringing together the IoP and IoS, along with the process and transaction of IoT data. For example, the IoT data from DIS (see Table 1 and 2 for definitions of abbreviations) connected to IoP and IoS, (representing systems of systems) enhances the cyber risk avoidance with real-time distribution and feedback directly from users and markets.

Thus, the evolution of IoT in the CPS space adds a new IoE perspective to the existing cyber risk avoidance mechanisms. The inter-relationships between these elements are crucial for defining a secure-by-default framework for I4.0. The current approaches taken for I4.0 assume development of IoP and IoS and reliability of IoE. In particular, a deeper understanding of the relationship between IoE and I4.0, following the categories presented in Table 1 is required in order to develop a new comprehensive cyber risk avoidance structure.

Furthermore, Table 2 shows that the next level of integration of CPS capabilities into the IoE is related to the integration of cyber physical capabilities into the industrial value chains (Hermann, Pentek, and Otto, 2016; Shafiq, Sanin, Szczerbicki, and Toro, 2015; Stock and Seliger, 2016; Wang et al., 2016). IoE uses principles of IoT and integrates network intelligence, providing convergence, orchestration and visibility across otherwise disparate systems (Hussain, 2017). The integration of CPS capabilities into IoE also provides a framework for the operation and management of multiple CPS-related elements in the context of I4.0. Figure 2 shows the inter-relationship between different CPS communities, processes, societies and platforms. The integration of cyber physical capabilities into the IoE, involves the integration of IoT, WoT, SM, IoP and IoS into SoS. The categories (derived from Table 1) are correlated in a hierarchical framework in Figure 2, to correspond with the integration taxonomy (in Table 2).

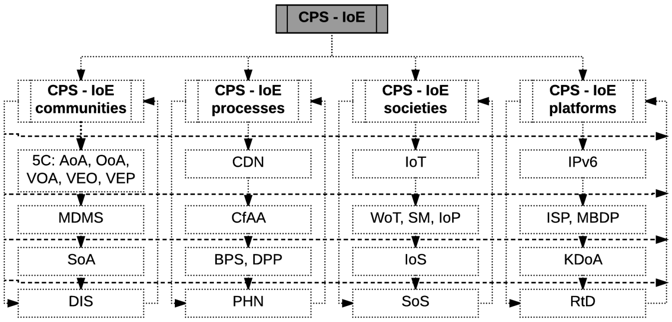

Figure 2: Hierarchical framework for integrating CPS into IoE, derived from this study

The framework for integrating CPS into IoE represents the starting point for building a new theoretical model for the 5C architecture in I4.0. The visualisation of system complexity facilitates that theoretical development and its understanding of interconnected concepts – both being crucial given that there is no direct reference in literature to the integration of IoE in I4.0.

3.4 Focus areas for integrating CPS-IoE for I4.0 in 5C

CPS architectures represent a very broad concept (Madakam, Ramaswamy, and Tripathi 2015, Leitão, Colombo and Karnouskos, 2016). The most pressing point for CPS is perhaps security (Zhu, Rieger, and Basar, 2011; Hahn et al., 2013). Risk management strategy for espionage, theft, or terrorist attacks, requires electronic and physical security that relates physical and engineered systems (Rajkumar et al., 2010; Leitão, Colombo and Karnouskos, 2016) to protect from insider threats, including interception and analysis of non-communications electromagnetic radiations (USDA, 2001; CoNSS, 2010; Olzak, 2013; DiMase et al., 2015).

Security requires information assurance and data security, protection for data in transit from physical and electronic domains and storage facilities (Longstaff and Haimes, 2002; CoNSS, 2010; Wahlster et al., 2013; DiMase et al., 2015; Marwedel and Engel, 2016; Toro, Barandiaran, and Posada, 2015). Asset management and access control are required for granting or denying requests to information and processing services (CoNSS, 2010; Rajkumar et al., 2010; Evans and Annunziata, 2012; DiMase et al., 2015), especially because CPS will interface with nontechnical users and influence across administrative boundaries is possible (Rajkumar et al., 2010). A process is needed to address novel vulnerabilities caused by life cycle issues, diminishing manufacturing sources, and the update of assets (DiMase et al., 2015), -- including system dynamics across multiple time-scales (Rajkumar et al., 2010; Marwedel and Engel, 2016), similar to loosely time-triggered architectures (Benveniste, 2010; Benveniste, Bouillard, and Caspi, 2010) and structure dynamics control (Sokolov and Ivanov, 2015).

Furthermore, CPS require anti-counterfeit and supply chain risk management to counteract malicious supply-chain components modified from their original design to enable disruption or unauthorised function (Evans and Annunziata, 2012; DiMase et al., 2015, Radanliev 2014a,b, 2015a,b,c,d 2016a). Standardisation of design and process (Sangiovanni-Vincentelli, Damm, and Passerone, 2012; Weyer et al., 2015) and hyper-connectivity in the digital supply chain (Ruan, 2017) also need to be supported. It is also suggested that limiting source code access to crucial and skilled personnel can provide software assurance and application security and may be necessary for eliminating deliberate flaws and vulnerabilities in the CPS (CoNSS, 2010; Rajkumar et al., 2010; DiMase et al., 2015). But this position is contested in the security community.

Security should be supported with forensics, prognostics, and recovery plans, for the analysis of cyber-attacks and coordination with other CPSs and those that identify external cyber-attack vectors (DiMase et al., 2015). An internal track and trace network process can assist in detecting or preventing the existence of weaknesses in the logistics security controls (DiMase et al., 2015). To support this, a process for anti-malicious and anti-tamper system engineering is needed to prevent CPS vulnerabilities identified through reverse engineering attacks (DiMase et al., 2015). The CPSS-5C architecture areas of focus in Figure 2 will support a robust integration of the 5C architecture (Lee, Bagheri, and Kao, 2015) and of virtual object architectures (Giordano, Spezzano, and Vinci, 2016) into CPSS for Industry 4.0 (Wahlster et al., 2013), so that cyber and physical components and connectors constitute the entire system at runtime (Bhave et al., 2010).

Glossary of acronyms 2: CPSS-AoF for integrating CPS-IoE in 5C for I4.0	
CPS security	**CPSS**
Areas of focus	**AoF**
5C architecture	**5C**
Electronic and physical security	EaPS
Information assurance and data security	ISaDS
Asset management and access control	AMaAC
Life cycle and anti-counterfeit	LCM
Diminishing manufacturing sources, material shortages and supply chain risk management	SCRM
Software assurance and application security	SAAS
Forensics, prognostics, and recovery plans	FRP
Track and trace	TaT
Anti-malicious and anti-tamper	AMAT

Table 3: CPSS - areas of focus (AoF) derived from this study for integrating CPS-IoE in 5C cyber security architecture

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

for I4.0

The CPSS-5C focal areas emphasize the need for security and privacy (Rajkumar et al., 2010; Zhu, Rieger, and Basar, 2011) and lead to the conclusion that in order to prevent continuation of CPS cyber-attacks, fast cyber-attack reporting and shared databases should be developed (Wahlster et al., 2013; DiMase et al., 2015). The systematic analysis is applied to each focal area to determine the inter-relationships between emerging cyber security concepts.

3.5 Requirements for the I4.0 for manufacturing and servitization.

Servitization in the context of I4.0 refer to predictive maintenance, forecasting machine failure, and intelligent machine-learning algorithms that are taking information from the Industrial IoT sensors and platforms to automatically diagnose failures and provide the remaining useful life of machinery. Here we are applying the grounded theory method to group the requirements for I4.0 servitization in manufacturing.

Electronic and physical security

This requires real-time data acquisition and storage solutions (Shi et al., 2011; Niggemann et al., 2015; Marwedel and Engel, 2016; Almeida, Santos and Oliveira, 2016) for fleets of machines (Wan et al., 2013), providing adaptive analysis, and peer-to-peer monitoring (Lee, Bagheri, and Kao, 2015).

Information assurance and data security

This needs to be supported with autonomous cognitive decisions, machine learning algorithms and high performance computing or data analysis (Wan et al., 2013; Niggemann et al., 2015; Pan et al., 2015), supported with fast cyber-attack information sharing and reporting via shared database resources (Wahlster et al., 2013; DiMase et al., 2015).

Asset management and access control

In I4.0, this requires that machines evolve into Cyber-Physical Production Systems (Weyer et al., 2015).

Life cycle and anti-counterfeit

This needs task-specific human machine interfaces (Wan et al., 2013; Niggemann et al., 2015; Marwedel and Engel, 2016), for self-aware (Weyer et al., 2015) machines and components prognostics and health management (Lee, Bagheri, and Kao, 2015).

Diminishing manufacturing sources, material shortages and supply chain risk management

This is required for prioritising and optimising decisions with self-optimising production systems (Shafiq, Sanin, Szczerbicki, and Toro, 2015; Wan, Cai, and Zhou, 2015; Brettel et al., 2016), supported with production-planning computer visualisation, such as SCADA systems integration with Virtual Reality (Posada et al., 2015) for developing

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

the decision support system (Lee, Bagheri, and Kao, 2015).

Software assurance and application security

This requires a big data platform (Lee, Kao, and Yang, 2014; Niggemann et al., 2015; Hussain, 2017) for sensors condition based monitoring (Lee, Bagheri, and Kao, 2015). Such platforms can enable complex models, such as cyber city designs (Petrolo, Loscri, and Mitton, 2016) using structured communications for mobile CPS (Almeida, Santos and Oliveira, 2016), cross-domain end-to-end communication among objects, and cloud computing techniques.

Forensics, prognostics, and recovery plans

This needs to be informed by key performance indicators (Bauer, Hämmerle, Schlund, and Vocke, 2015).

Track and trace

Feedback and control mechanisms (Niggemann et al., 2015) are required for enabling supervisory control of actions, to avoid or grant required access or to design a resilient control system (Lee, Bagheri, and Kao, 2015).

Anti-malicious and anti-tamper

This would be facilitated with loosely time-triggered architectures (Benveniste, 2010; Benveniste, Bouillard, and Caspi, 2010) and structure dynamics control (Sokolov and Ivanov, 2015).

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:	

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

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 4: Grouping of concepts for individual levels of the 5C architecture - derived from this study

3.6 Proposed new 5C architecture in I4.0

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

We propose a new 5C architecture in I4.0, which includes: (1) self-maintaining machine connection for acquiring data and selecting sensors; (2) self-awareness algorithms for conversion of data into information (similar to Lee, Kao, and Yang, 2014; Toro, Barandiaran, and Posada, 2015; Weyer et al., 2015); (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 (similar to Brettel et al., 2016); (5) configuration feedback and supervisory control from cyber space to physical space, allowing machines to self-configure, self-organise and be self-adaptive.

Connection	SAAS	BDP, mCPS	CBM	Self-maintain
Conversion	LCM	HMI, MaC	PHM	Self-aware
	AMAT	LTTA, SDC		
Cyber (analytic solutions)	EaPS	RTD, FoM, AA, PtPM	CPS	Self-compare
Cognition	SCRM	POD, SOPS	DSS	Self-predict
	ISaDS	ACD, MLA, HPC, ISR		Self-optimise
Configuration	TaT	CoA	RCS	Self-organise
	FPR	KPI		
	AMaAC	CPPS		Self-configure

Table 5: The applications and technologies related to the IIoT in individual levels of the 5C architecture derived from this study

The emerging applications and technologies in Table 5 are presented in the form of a hierarchical cascading model in Figure 3 in order to visualise their relationships in the 5C architecture for I4.0. Figure 3 presents the way machines can connect to the 5C architecture and exchange information through cyber network (Toro, Barandiaran, and Posada, 2015) and provide optimised production and inventory management (Lee, Bagheri, and Kao, 2015; Wan, Cai, and Zhou, 2015; Weyer et al., 2015) and CPS lean production (Kolberg and Zühlke, 2015).

The categorisation in Table 5 derived from applying grounded theory to categorise concepts in existing literature. The principles of grounded theory demand that all prominent themes need to be categorised, hence the emergence of the 'cyber' category. However, from a cyber security engineering perspective the 5C model in Section 5 is fundamentally flawed, referring to the middle layer as 'cyber' demonstrates a poor understanding in literature of current developments in industrial systems and the fact that cyber elements now extend from sensor/actuator through to supervisory control and advanced analytic solutions. The principles state that we need to report what we observe, not what we think its

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

correct or incorrect and since cyber is a buzz word, it can refer to many things. It is probably incorrect to use in this context, but the taxonomy is based on grounded theory and the fundamental principles of grounded theory are applied to categorise themes from existing literature.

Nevertheless, the described new 5C architecture for I4.0 also represents cognitive architecture. The cognitive architecture allows for learning algorithms and technologies to be changed quickly and re-used on different platforms (similar to Niggemann et al., 2015; Brettel et al., 2016), which is necessary in usual I4.0 situations, such as, to create multi-vendor and modular production systems (as recommended by Weyer et al., 2015). Such re-using can be achieved through VEO and VEP in CPS, which enable the real-time synchronised coexistence of the virtual and physical dimensions (as recommended by Shafiq, Sanin, Szczerbicki, and Toro, 2015). The emergence of cyber cognition, confirms that CPS design requires multi-discipline testing and verification, including: system design, system engineering and policy design (similar to Balaji et al., 2015), and requires understanding of system sociology (Dombrowski and Wagner, 2014). The proposed 5C architecture operates in a similar method with social networks, in the sense that individuals can influence the production line (recommended by Bauer, Hämmerle, Schlund, and Vocke, 2015; Wan, Cai, and Zhou, 2015).

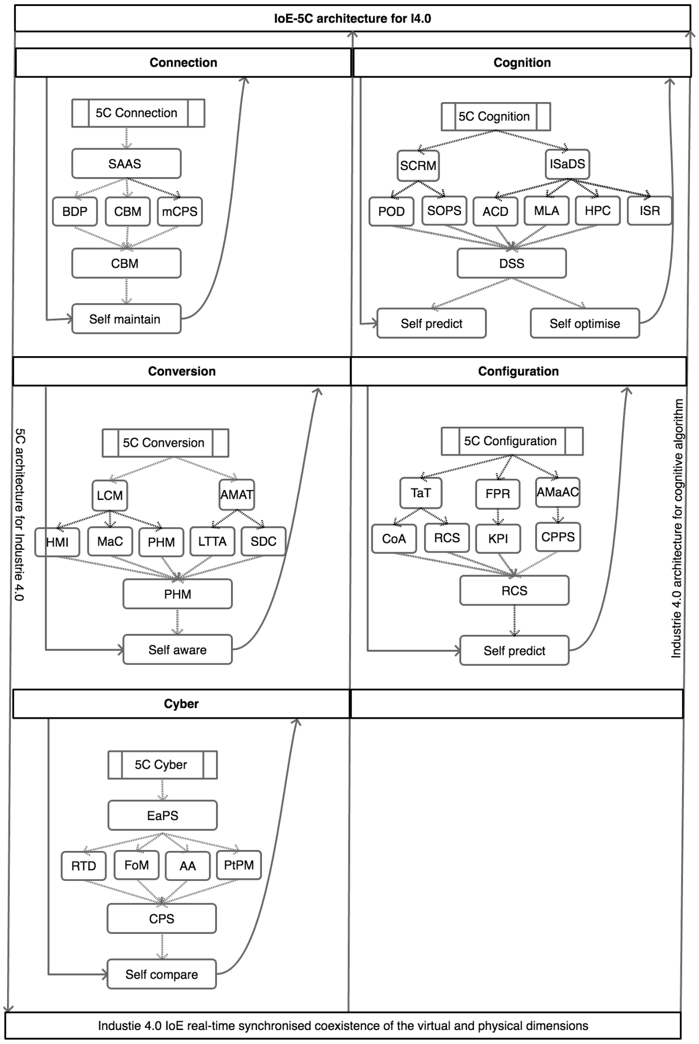

Figure 3: Cascading model deriving from this study - IoE-5C architecture for I4.0

4. Vision for CPS-IoE integration in Industry 4.0

CPS security is essential for industrial competitiveness and for harnessing economic value of the digital industry (Rajkumar et al., 2010; Brettel et al., 2016; Leitão, Colombo and Karnouskos, 2016; Stock and Seliger, 2016; Wang et al., 2016). The future vision of CPS integration in the IoT includes instruments and processes to enable energy-aware buildings and cities (EABaC) (Balaji et al., 2015; Marwedel and Engel, 2016; Weyer et al., 2015); physical critical infrastructure with preventive maintenance (CIPM), and self-correcting cyber-physical systems (SCCPS) themselves (Rajkumar et al., 2010; Zhu, Rieger, and Basar, 2011; Brettel et al., 2016; Leitão, Colombo and Karnouskos, 2016). In addition, the electric power grid represents one of the largest complex interconnected networks (Hahn et al., 2013). Under stressed conditions, single failure can trigger complex cascading effect, creating wide-spread failure and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

blackouts (Rajkumar et al., 2010). Flexible AC Transmission Systems would enable protection against such cascading failures (Rajkumar et al., 2010). Distributed energy resource technologies (Ahmed, Kim, and Kim, 2013; Marwedel and Engel, 2016) such as wind power, create additional stress and vulnerabilities. Advanced power electronics and energy storage are required for here for coordination and interactions (Rajkumar et al., 2010; Leitão, Colombo and Karnouskos, 2016; Marwedel and Engel, 2016).

4.1 Present challenges for CPS-IoE in I4.0

For CPS and IoE in I4.0, present industrial techniques are: Robustness, Safety, and Security (Zhu, Rieger, and Basar, 2011; Hahn et al., 2013); Control and Hybrid Systems (Shi et al., 2011; Leitão, Colombo and Karnouskos, 2016); Computational Abstractions Architecture (Rajkumar et al.,2010; Wahlster et al., 2013; Madakam, Ramaswamy, and Tripathi 2015); Real-Time Embedded Systems Abstractions (Tan, Goddard, and Pérez, 2008; Shi et al., 2011; Kang and Kapitanova, 2012; Leitão, Colombo and Karnouskos, 2016; Marwedel and Engel, 2016); Model-based Development (Rajkumar et al., 2010; Bhave et al., 2011; Jensen, Chang, and Lee, 2011; Shi et al., 2011; Wahlster et al., 2013); and Education and Training (Rajkumar et al., 2010; Wahlster et al., 2013; Faller and Feldmüller, 2015). However, as the integration of CPS into I4.0 is an evolutionary process (Wahlster et al., 2013), the techniques within the topics and techniques above will be changing with time, which requires flexibility management of the complexities of the CPS. In addition to these techniques, for creating a reliable, secure and economically sustainable power system, financial planning arrangements should be developed for buyers and sellers in the renewables electricity market (Rajkumar et al., 2010; Ahmed, Kim, and Kim, 2013). Finally, CPS applications such as Sentinel (Balaji et al., 2015) can be used to exploit the information flow for energy savings.

4.2 Future techniques for CPS-IoE in I4.0

Building upon the present techniques, the deployment of self-sustaining networked sensors and actuators (Rajkumar et al., 2010) should be in symbiotic relations with the physical environment (Pan et al., 2015). Such 5C vision could be modelled through a user-centric Cloud (Gubbi et al., 2013). There are also important environmental techniques associated with cloud computing (e.g. Greenpeace International, 2011; Greenpeace International, 2012). Environmental natural resources are crucial in sustaining economic development (Stock and Seliger, 2016), and CPS in I4.0 should be focused on creating eco-industrial by-product synergy (Pan et al., 2015).

Another future challenge is the evolution of I4.0 into self-adapting 5C, by moving from centralised-federated to decentralised-integrated architecture. This process would present a new vision for distributed (Wan, Cai, and Zhou, 2015) and integrated-decentralised (Stojmenovic, 2014) multi-agent swarm intelligence, based on cooperation of large population of simple agents. The decentralisation of the control function to a multi agent swarm – which implies lack of central control dictating individual behaviour and interactions among swarm agents – stimulates the emergence of intelligent global behaviour. Individual agents exploit cloud services to analyse, predict, optimise and mine scalable capabilities of historical data and enable applications to self-adjust their behaviour to self-optimise their own performance (Shafiq, Sanin, Szczerbicki, and Toro, 2015; Brettel et al., 2016). In such decentralised systems, individual agents' 'contract-based design' is applied before 'platform-based design' (Sangiovanni-Vincentelli, Damm, and Passerone, 2012). Contract-based design enables actor-oriented design of multiple models of computation to be integrated in a single hierarchical system (Bhave et al., 2011), similar to loosely time-triggered architectures (Benveniste, 2010) but applied to I4.0.

This review presents different groups of things, and a form of dependency or a causal edge relation between them. Table 4 shows the edges between different nodes representing groups of the influence of future and present techniques on the vision for CPS-IoE integration in I4.0.

Glossary of acronyms 4: **Grouping of future and present techniques**	
Present techniques	
Education and Training	EaT
Financial planning	FP
Information flow for energy savings	IFfES
Robustness, Safety, and Security	RSS
Control and Hybrid Systems	CHS
Computational Abstractions Architecture	CAA
Real-Time Embedded Systems Abstractions	RTESA
Model-based Development	MBD
Future techniques	
Eco-industrial by-product synergy	EIS
Distributed integrated-decentralised	DID
Multi-agent swarm intelligence	SI
Contract-based design	CBD
Self-sustaining networked sensors	SSS
Symbiotic relations with the physical environment	SRPE

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

User-centric Cloud based vision	CCV
Future vision for CPS-IoE integration in Industry 4.0	
Energy-aware buildings and cities	EABaC
Critical infrastructure with preventive maintenance	CIPM
Self-correcting of cyber-physical systems	SCCPS
Flexible AC Transmission Systems	FACTS
Distributed energy resource technologies	DER

Table 6: Grouping of future and present techniques on the future vision for CPS-IoE-5C in I4.0 derived from this research

While I4.0 refers to IoP and IoS, it does not include the IoE in the proposed 5C architecture. The groups (in Table 4) represent a form of conceptual grouping model for building upon 5C architecture in Figure 1 (Lee, Bagheri and Kao, 2014), but separates the future techniques from the present techniques. This separation constitutes the grounding for the empirical review of the national I4.0 initiatives discussed in Section 4.1 and summarized in the empirical review (Tables 7-9).

4.3 Review of global I4.0 frameworks and initiatives

Following the systematic review of academic literature on I4.0, this section represents and empirical review of the world leading digital industry frameworks in this space. The aim of this section is to relate the academic literature and industry reports, with what is happening in practice. The first objective of the empirical review is to determine whether the practical frameworks and initiative globally are implementing the recommendations from the state of the art leading research in this area. The second objective is to relate the state of the art research with the leading frameworks and initiatives and to build a reference architecture for the integration of the emerging categories from the taxonomic review, with the implementation of these concepts in the I4.0 frameworks.

The empirical review starts with Industrie 4.0 (GTAI, 2014; Industrie 4.0, 2017) as the world leading initiative for I4.0 and follows with a systematic empirical review of (additional 13) I4.0 world leading initiatives. The main elements of each world leading initiative in Table 3 are separated in: areas of focus, areas of decision and areas of action. The complete systematic empirical review identifies a number of shortcomings in individual initiatives, which are complimented by other initiatives. This required building a model that integrates the strengths and reduces the weaknesses of all initiatives. There are problems, when, for example, some of the areas of focus, decision and action differ in terms of strategy and propose very different approaches. To resolve this issue, we use two strategies. Firstly, the individual areas as categorised in the systematic empirical review (Table 3) are used as reference categories. Secondly, the categories in Table 3 are used for building the I4.0 architecture model in Figure 4 that relates various areas to each other and eliminates conflicts in different and sometimes contrasting I4.0 approaches.

The main elements of each initiative are separated in: areas of focus, areas of decision and areas of action (Table 7-9). However, the compelling of data into these categories is quite challenging, as some initiatives, for example, represent a collection of descriptive explanations and do not provide explicit areas of focus, decision and action. The systematic analysis of the world leading initiatives (outlined in Table 7), presents some of the complexities in developing a unifying architecture, with a step-by-step method for I4.0-5C integration of CPS capabilities into IoE. Some world leading initiatives have explicitly developed strategies for digital architectures; e.g. the Industrial Internet Consortium (IIC, 2017); Industrie 4.0 (GTAI, 2014; Industrie 4.0, 2017). Other world leading initiatives focus on loosely defined standards that emerge from forums, such as in the case of Industrial Value Chain Initiative (IVI, 2017); or blogs, in the case of Made Different (SA, 2017); or surveys, in the case of High Value Manufacturing Catapult (John, 2017); or even direct electronic open submission of recommendations for changing or editing the strategy, such as the National Technology Initiative (ASI, 2016).

Some initiatives promote activities in the format of workgroups (IVI, 2017), while other initiatives promote activities in the format of testbeds (IIC, 2017) or digital catapults (John, 2017). From the empirical analysis in Table 7, the direction of the I.40 architecture is geared by activities, such as, workgroups and testbeds in the case of Industrie 4.0 (GTAI, 2014) and are supported by economic and financial digital catapults, (e.g. the UK Catapult programme). Furthermore, the Fabbrica Intelligente (MIUR, 2014) and Industrie 4.0 (GTAI, 2014) initiatives focus on promoting key project in the digital industry; the Industrial Internet Consortium (IIC, 2017) focuses on promoting key IIoTindustries; and the New France Industrial (NIF, 2013), the High Value Manufacturing Catapult (John, 2017) and the National Technology Initiative (ASI, 2016) focus on promoting the development of key technologies. Made in China 2025 initiative (SCPRC, 2017) promotes key tech sectors, while the Made Different initiative (SA, 2017) promotes key transformations. The diversity of the approaches in world initiatives grows in magnitude as the systematic empirical analysis advances to the less evolved (Table 8) and the elusive initiatives (Table 9).

Leading I4.0 national initiatives			
I4.0 national frameworks	**Category 1: Areas of focus**	**Category 2: Areas of decision**	**Category 3: Areas of action**
Germany - Industrie 4.0	**Workgroups – I4.0 policy:** (1) The Smart Factory; (2) The	**Relationships – I4.0 principles:** (1) based on CPS, IoT and Cloud	**Priority areas – I4.0 mission/vision - the Smart Service 5 priority areas:**

(GTAI, 2014)	Real Environment; (3) The Economic Environment; (4) Human Beings and Work; (5) The Technology Factor. **Techniques:** (1) IT security; (2) Reliability and stability; (3) Integrity of production processes; (4) Avoidance of IT snags; (5) Protect industrial knowhow; (6) Lack of adequate skill-sets; (7) Reluctance to change; (8) Loss of jobs.	Computing. **5C imperative element - 6C system:** (1) Connection; (2) Cloud; (3) Cyber; (4) Content/context; (5) Community; (6) Customisation. **5C design building blocks for I4.0 - 4 key design principles:** (1) Interoperability; (2) Information transparency; (3) Technical assistance; (4) Decentralised decisions.	(1) Integrated Production and Service Innovation; (2) Internet and Service Economy; (3) Technological Enablers; (4) Business Organisation Requirements; (5) Innovation-oriented Framework **5C key testbeds for I4.0 technologies -** Industrie 4.0 research into practice, over 500 projects are being carried out in Germany (Industrie 4.0., 2017).
USA - (1) Industrial Internet Consortium (IIC, 2017); (2) Advanced Manufacturing Partnership (AMP, 2013).	**5C key industries for I4.0 - IIC industries:** (1) Energy; (2) Healthcare; (3) Manufacturing; (4) Smart Cities; (5) Transportation. **AMP focus programmes - AMP policy:** (1) NIST Manufacturing USA Programme; (2) National Network for Manufacturing Innovation Programme; (3) NIST Advanced Manufacturing Technology Consortia (AMTech) programme. **5C imperative element - AMP areas of interest:** (1) Advanced Sensors, Controls, Platforms, and Modelling (ASCPM); (2) Visualisation, Informatics, and Digital	**IIC output - principles:** (1) Industrial Internet of Things Connectivity Framework (IICF); (2) Industrial Internet Reference Architecture v 1.8. **5C design actions for I4.0 - AMP goals:** (1) Increase the competitiveness of U.S. manufacturing; (2) Facilitate the transition of innovative technologies into manufacturing; (3) Accelerate the development of an advanced manufacturing workforce; (4) Support sustainable business models.	**5C key testbeds for I4.0 technologies - IIC testbeds:** 22 Testbeds to be deployed for the Industrial Internet; **Priority areas - AMP snapshot of priority technology areas - AMP mission/vision:** (1) Advanced materials manufacturing; (2) Engineering biology to advance bio-manufacturing; (3) Bio-manufacturing for regenerative medicine; (4) Advanced bio-products manufacturing; (5) Continuous manufacturing of pharmaceuticals

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

	Manufacturing Technologies (VIDM) (Edgar and Davis, 2015).		
UK – (1) Catapults (John, 2017); (2) UK Digital Strategy (DCMS, 2017).	**Priority area – DC mission/vision:** Catalyst for sustainable high value manufacturing. **Measured area of impact:** Economic impact. **5C design actions for I4.0 - areas of focus:** (1) Technology readiness; (2) UK policy; (3) Funding from 3 sources: public funding, business contracts, collaborative projects.	**5C design building blocks for I4.0 - design elements:** (1) Open access facilities; (2) Contractual agreements; (3) Intellectual property and confidentiality; (4) State aid compliance; (5) Financial support; (6) Publicity. **I4.0 focus - principles:** (1) Survey; (2) Industrial strategy consultation.	**5C key testbeds for I4.0 technologies - catapults: (1)** 11 Digital Catapult centres - including HVM network of another seven centres, (**5C key technologies for I4.0)** (2) 27 Key technologies **5C key projects for I4.0 -** Manufacturing catapult 7 Key projects: 7 HVM Catapult centres (John, 2017). **Digital Strategy:** (1) Connectivity; (2) Digital skills; (3) Digital sectors; (4) Wider economy; (5) Cyber security; (6) Digital government; (7) Data economy.
Japan - (1) Industrial Value Chain Initiative (IVI, 2017); (2) New Robot Strategy (NRS) (METI, 2015) and RRI (METIJ, 2015).	**5C design building blocks for I4.0 - IVI loosely defined standards:** (1) Industrial Value Chain Reference Architecture (IVRA); (2) IVI Platform for Smart Manufacturing Ecosystem (IVI, 2017); (3) Smart Manufacturing Business Scenarios (IVI, 2016). **NRS pillars - 5C imperative element:** (1) Robots innovation hub; (2) Robot society; (3) Robotics in IoT. **NRS areas of focus:** (1) AI learning from big-data; (2) AI	**Relationship - IVI strengths/principles:** (1) Gathers a broader understanding of more general connection models (reference models); (2) Aims to design 'loosely defined standard', as an adaptable model instead of a rigid system. **5C design actions for I4.0 - NRS objectives:** (1) AI reasoning; (2) AI learning; (3) AI intelligence infrastructure.	**IVI Activities - policy:** (1) IVI Forum; (2) 25 Business Scenario Workgroups (BSWGs); (3) 8 Platform Workgroups (PWGs). **Priority areas - NRS mission/vision:** (1) Robots autonomy; (2) Robot as information terminals; (3) Robotic networking. **5C key technologies for I4.0 - NRS core technologies:** (1) Artificial intelligence; (2) Automated behaviour.

	reasoning from existing knowledge; (3) AI brain.		
France - New France Industrial (NFI) – also known as: la Nouvelle France Industrielle or Industry of the Future (NIF, 2013).	**5C key markets for I4.0 - key Markets - 9 solutions:** (1) Data economy; (2) Smart objects; (3) Digital trust; (4) Smart food production; (5) New resources; (6) Sustainable cities; (7) Eco-mobility; (8) Medicine of the future; (9) Transport of tomorrow	**NIF policy:** (1) Subsidies or repayable advances; (2) Tax incentives; (3) Loans; (4) SME business modelling support; **Priority areas – Pillars - NIF mission/vision:** (1) Developing cutting edge technologies; (2) Helping companies adapt to the new paradigm; (3) Training employees; (4) Showcasing the French industry of the future; (5) Strengthening European and international cooperation.	**5C key technologies for I4.0 - key technologies:** List of 47 key technologies that need to be industrialised in the 9 solutions. **5C imperative element:** NFI economy of data: (1) Digital technology, virtualisation and the Internet of Things; (2) Cobotics, augmented reality; (3) Additive manufacturing (3D printing); (4) Monitoring and control; (5) Composites, new materials and assembly; (6) Automation and robotics; (7) Energy efficiency (NIF, 2013).

Table 7: Empirical review of world leading digital industry (I4.0) frameworks

Emerging I4.0 national initiatives			
I4.0 national frameworks	**Category 1: Areas of focus**	**Category 2: Areas of decision**	**Category 3: Areas of action**
Nederland - Smart Industry; or Factories of the Future 4.0 (Bouws, et.al., 2015).	**Priority areas - SI mission/vision:** (1) Defining strategic objectives; (2) Defining activities within the smart industry agenda; (3) Defining implementation.	**Relationship - principles:** (1) SWAT analysis; (2) Developed a 'dare to share' data cooperation initiative.	**5C design building blocks for I4.0 - key contribution:** (1) Demonstrates illustrative projects; (2) Demonstrates data sharing initiatives; (3) Developed action objectives, agenda and plan on standardisation; (4) Developed action line on cyber security.
Belgium - Made Different (SA, 2017).	**Priority areas - Human centred dynamic production - MD mission/vision:** (1) High value market responsive manufacturing;	**Relationship - principles:** (1) Based on CPS; (2) blog (forum); (3) Focused on products and services with high added value.	**5C design building blocks for I4.0 - promotes 7 crucial transformations:** (1) World Class Manufacturing Technologies; (2) End-

	(2) New business models and digitised production; (3) On demand resilient production system; (4) CPS; (5) Circular economy; (6) Reduce materials and energy consumption.	**5C design actions for I4.0 - activities:** (1) Blog (forum); (2) Factory of the future case studies.	to-end Engineering; (3) Digital Factory; (4) Human Centred Production; (5) Production Network; (6) Eco Production; (7) Smart Production Systems.
Spain - Industrie Conectada 4.0 (MEICA, 2015).	**Priority area - area of focus: IC mission/vision** Linking the physical to the virtual to create intelligent industry.	**Principles:** (1) Based on CPS; **Policy:** (2) Financial support for digital transformation; (3) Personalised advice for SMEs; **Relationship:** HADA - Advanced Self-diagnosis tool.	**5C design building blocks for I4.0 - promotes:** (1) Hybridisation between the physical and digital worlds; (2) Digital transformation for the evolution to the digital economy.
Italy - Fabbrica Intelligente (MIUR, 2014).	**Priority areas - areas of focus - FI mission/vision:** Developing and implementing a strategy for (1) Transforming towards new product, services, process, and technologies; (2) Design, execution and enhancements of research results; (3) Connecting nation and regional research with international policies; (4) Improving possibilities for using EU funds.	**5C design building blocks for I4.0 - design activities:** (1) Realisation of research projects; (2) Technology transfer, sharing of knowledge and networking; (3) Sharing research infrastructure; (4) Support and facilitation of smart and sustainable entrepreneurship; (5) Support for technological forecasting activities in the smart factory sector; (6) Support for the growth of the human capital.	**5C key projects for I4.0 - 4 Key projects:** (1) Sustainable manufacturing; (2) Adaptive Manufacturing; (3) Smart Manufacturing 2020; (4) High Performance Manufacturing.

Table 8: Empirical review of less evolved digital industry (I4.0) frameworks

Roughly defined I4.0 national initiatives			
I4.0 national frameworks	**Category 1: Areas of focus**	**Category 2: Areas of decision**	**Category 3: Areas of action**
China - Made in China 2025 (SCPRC, 2017)	**Priority area - mission:** Comprehensive upgrade of the Chinese industry. **Guiding principles - MiC**	**Role of the state - policy:** (1) Provide an overall framework, (2) Utilising financial and fiscal tools, and supporting the	**5C key tech sectors for I4.0 - 10 priority tech sectors:** (1) New advanced information technology; (2) Automated machine tools & robotics;

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

	mission/vision: (1) Innovation-driven manufacturing; (2) Quality over quantity; (3) Green development; (4) Optimise the Chinese industry infrastructure; (5) Nurture human talent. **Difference - principles:** (1) Focus on the entire manufacturing process and not just innovation; (2) Promotes the development of advanced and traditional industries and modern services; (3) Less focus on state involvement, and market mechanisms are more prominent; (4) Clear and specific measures for innovation, quality, intelligent manufacturing, and green production.	creation of manufacturing innovation centres (15 by 2020 and 40 by 2025). **5C design building blocks for I4.0 - role of the industry:** (1) Strengthening intellectual property rights; (2) Protection for small and medium-sized enterprises (SMEs); (3) Allowing companies to self-declare their own technology standards; (4) Help companies participate in international standards setting.	(3) Aerospace and aeronautical equipment; (4) Maritime equipment and high-tech shipping; (5) Modern rail transport equipment; (6) New-energy vehicles and equipment; (7) Power equipment; (8) Agricultural equipment; (9) New materials; and (10) Biopharma and advanced medical products.
G20 - New Industrial Revolution (NIR) (G20, 2016)	**Priority area - NIR mission/vision:** Promoting joint action by enhancing existing communication and collaboration mechanisms. **NIR principles**: develop multi-stakeholder communication principles within and across countries.	**Policy key point - policy:** (1) Trade liberalisation and the elimination of subsidies.	**5C design actions for I4.0 - actions:** (1) Research collaboration; (2) The role of SMEs; (3) Employment and workforce skills; (4) Cooperation on standards; (5) New industrial infrastructure; (6) Intellectual property rights protection; (7) Industrialisation in developing countries.
Russia - National Technology Initiative (NTI) (ASI, 2016).	**Priority areas – NTI mission/vision:** (1) Identifying new markets; (2) Identifying key technologies. **Guiding key principle:** Focus is on market creation as opposed to technology development.	**Policy key point - policy:** Promote market demand, new technological standards and national cyber security; **5C design building blocks for I4.0 - strength:** Electronic open submission of recommendations	**5C key tech networks for I4.0 - key technologies:** 13 key tech examples. **5C key tech networks for I4.0 - set of market network: *transport system*** (1) AutoNet; (2) AeroNet; (3) MariNet - ***national security resources*** (4) SafeNet; (5)

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

		for changing or editing the strategy.	EnergyNet; (6) FoodNet - ***technological changes*** (7) HealthNet; (8) NeuroNet; and (9) FinNet.

Table 9: Empirical review of elusive digital industry (I4.0) frameworks

The differences in these approaches correspond to the different national and international strengths and aspirations of the promoters of these strategies. The empirical review (Table 7-9) summarize different and often conflicting approaches that harden adoption of coherent standards for I4.0 architecture.

To simplify these confusing differences in areas of focus, some of the different areas of focus, decision and action in the world leading initiatives can be grouped based on similarities in the key technologies: NIF lists 47 key technologies, Made in China 2025 prioritizes 10 tech sectors and NTI includes 13 key tech examples. However, some initiatives focus on areas of decision and action that differ greatly from the main objectives of other initiatives. For example, the focus on market networks and market creation of the National Technology Initiative (ASI, 2016) is opposed to the mainstream technology development in NIF that includes policies for subsidies and repayable advances, tax incentives and loans.

These differences call for the development of an I4.0 architecture model for inter-relating the three areas of focus, decision and action in a meaningful method. The systematic analysis outlined in Table 3 provides detailed explanation of these areas. We develop the method accounting for this analysis into an I4.0 architecture model that is presented in Figure 4. This architecture model represents the process of building a coherent I4.0-5C reference architecture that integrates CPS capabilities into IoE. The proposed I4.0 architecture model enables a step-by-step review and adaptation of the different elements that emerge from the academic literature analysed and the 14 world leading I4.0 initiatives.

4.4 An I4.0 architecture model for the integration of CPS-IoE-5C into I4.0

The I4.0 architecture model in Figure 4 compensates for shortcomings in each of the individual world leading initiatives. For example, not all initiatives provide feedback mechanisms for policy development. Rather, the I4.0 architecture model derives with integrated policy recommendations and policy feedback mechanisms that are directly related to the 5C architecture for I4.0. The I4.0 architecture model in Figure 4 also makes direct recommendations for imperative

 doi:10.20944/preprints201903.0139.v1

elements of action as extracted from Table 3. This is happening in the context in which some of the initiatives, including Nederlands' Smart Industry, Belgium's Made Different, Spain's Industrie Conectada 4.0, Italy's Fabbrica Intelligente, UK's Manufacturing catapult, China's Made in China 2025, and Russia's National Technology Initiative all lack imperative elements of action in their I4.0 architectures.

The architecture model in Figure 4 addresses this issue through integrating best practices from the empirical analysis in Tables 7-9. Figure 4 represents the first I4.0 architecture model that integrates a state of the art academic literature (Figure 4:1, 4:2, 4:4) with the state of the art in I4.0 practical initiatives applied globally (Figure 4:3). The integration of models from academic literature with empirical study of I4.0 national initiatives, leads to a new set of techniques, such as the different approaches in national initiatives that imply particular national policies and standards and which are not discussed in the existing literature.

The model in Figure 4 presents and consolidates these techniques, building on the empirical study to integrate CPS-IoE into in 5C cyber security architecture for I4.0. The conceptual grouping model of future and present techniques on the vision for CPS-IoE-5C in the context of I4.0 presented in Table 4 and the I4.0 cascading model derived from academic literature presented in Figure 3 are then juxtaposed over the empirical study in Table 3.

The I4.0 world visions emerging from the world leading initiatives are aggregated in an attempt to make visible the potential integration areas. A comprehensive vision for the integration of CPS-IoE into 5C architectures for I4.0 requires consideration of all mission statements from each initiative presented in Tables 7-9. This holistic approach requires the formulation of encompassing principles for the integration of I4.0 across all initiatives (Figure 4:3).

The argument of this I4.0 architecture model is that the integration of CPS-IoE-5C into I4.0 is not a selective process. Rather, it requires the synchronisation and harmonisation between I4.0 architectures, which leads to standardisation of world leading visions. Such integration requires evaluation principles. The first stage of this study identified the evaluation principles from academic literature on CPS-IoE in 5C architecture models. Figure 4 consolidates the framework from Figure 2, with the AoF from Figure 2, the Cascading model from Figure 3 and the grouping model from Table 6. In the second stage, this process is shaped by the particular I4.0 world leading initiative that acts in each national context. We suggest that each particular I4.0 world leading initiative should be considered prior to deciding whether the 5C reference architecture is adequate and corresponds to the individual national strategy.

For example, the German Industrie 4.0 initiative contains 6C architecture model: (1) Connection (sensor and networks); (2) Cloud (computing and data on demand); (3) Cyber (model & memory); (4) Content/context (meaning and correlation); (5) Community (sharing and collaboration); (6) Customisation (personalisation and value) (GTAI, 2014; Industrie 4.0, 2017). The findings from this study show that, in particular, one of the 6Cs – Community (sharing and collaboration), represents an entirely new SoS network. Hence, in this study the CPS-IoE-5C integration into I4.0 reference architecture refers basically to IoE as opposed to IoT. This means that I4.0 has evolved beyond the CPS-IoT-6C integration into I4.0. The German I4.0 strategy that includes the Community (sharing and collaboration) layer of the 6C was designed in 2013. At that time, IoT technology was emerging and tended to dominate the academic and industry research. However, the German I4.0 initiative goes beyond IoT and refers to IoP and IoS. Hence, despite the lack of direct reference to IoE, the integration of I4.0 into IoE is indirectly anticipated in the German I4.0 initiative. Therefore, the I4.0 architecture model proposed in our study represents an updated version of the German I4.0 initiative.

The integration of CPS-IoE-5C into I4.0 while minding the world leading principles requires also the alignment of I4.0 policies. The empirical study presented in Table 3 highlights gaps in some of the world leading policies. To address these gaps, the architecture model presented in Figure 4 outlines the most important policies that support the transformation of existing industries towards the integration of CPS-IoE-5C into I4.0. Thus, we propose an overarching architecture model for policy development that should be supported by clarification of the imperative elements of the 5C integration into the I4.0 as seen in Figure node 4:8 The imperative elements in the I4.0 architecture model (Figure node 4:8) are for reference purposes only, as they would differ depending on the particular business environment and the available support for the I4.0 as an infant industry. In economic theory, financial support in the form of direct subsidies is allowed for the support of infant industries. Hence, the level of support depends on the national government funding being made available.

The arrows in Figure 4, stand for the direction of the logical flow and are representing the integration processes of CPS-IoE-5C into I4.0.

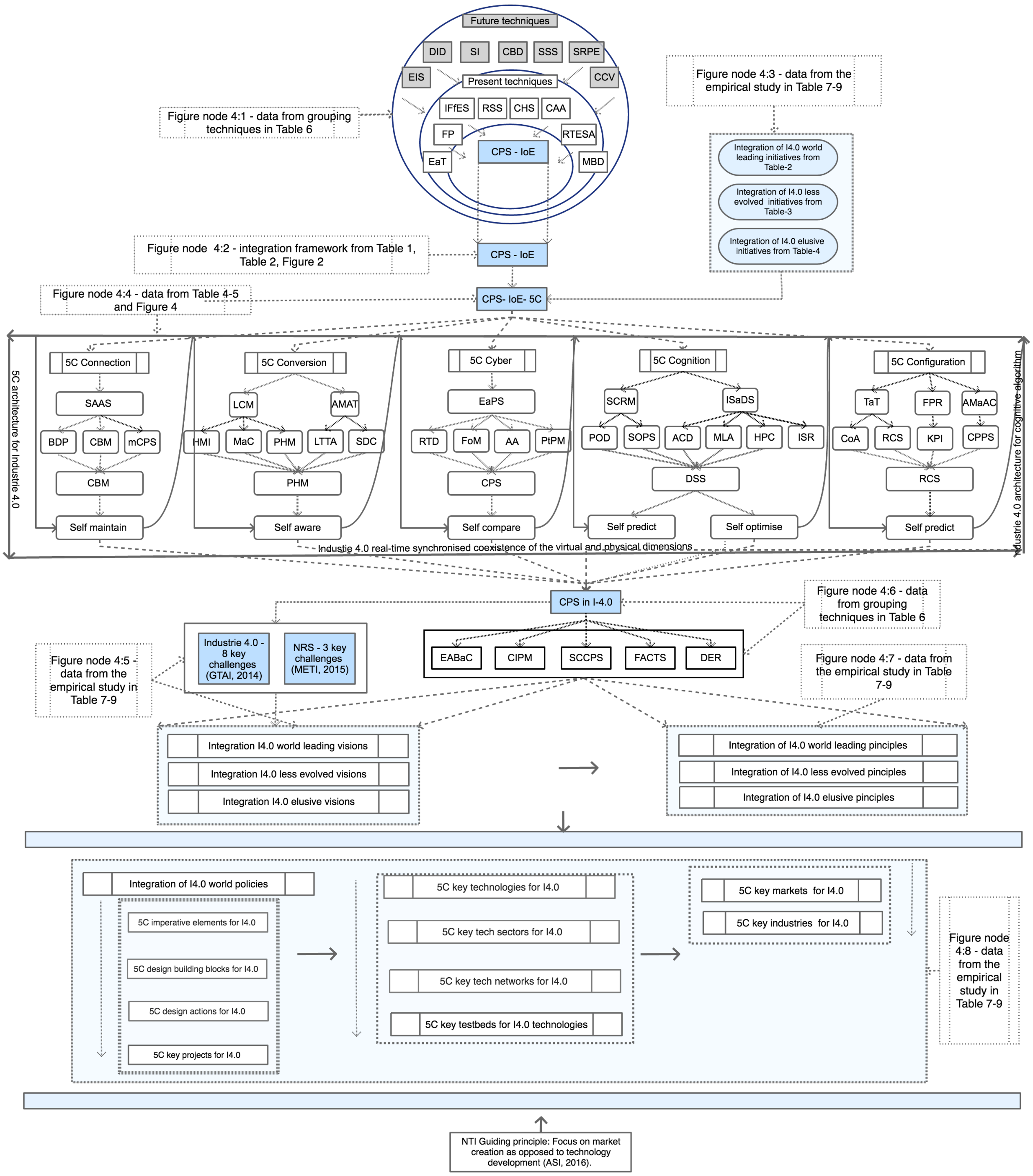

Figure 4: I4.0 architecture model for the integration of IIoT in the I4.0

 doi:10.20944/preprints201903.0139.v1

Through a systematic literature review and empirical study, we developed the I4.0 architecture model and explained how such integration could be achieved. This model is the result of a holistic method to integrate the world leading I4.0 initiatives into a logical sequence. 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 architecture model in this study provides a logical sequence that includes the NRS core technologies specification for the integration of AI and automated behaviour (METI, 2015; METIJ, 2015) in the NFI key technologies list.

While with the evolution of I4.0 in IoE, other elements of standardisation architecture will emerge, the current 5C building blocks for I4.0 (Figure 4:11) are extracted from the requirements of the imperative elements (Figure 4:10) as presented in the leading initiatives (Figure 4:3) and policies (Figure 4:9) for the harnessing of economic value and reducing the associated cyber risk, and should not be compromised.

The 5C imperative elements (Figure node 4:8) for the I4.0 are followed by the 5C design building blocks (Figure node 4:8) for I4.0. The 5C design building blocks represent more specific concepts in terms of I4.0 standardisation architecture and can serve as guidance and feedback mechanisms for the CPS-IoE-5C integration into I4.0. Building block concepts, such as: information transparency and open access facilities provide guidance to national regulators and industry network architects. The I4.0 architecture model provides feedback mechanisms from national strategies towards standardisation strategy while building blocks. For example, one feedback mechanism could be the NTI's initiative (ASI, 2016) to build a block for electronic open submission of recommendations for changing or editing. Some of the building blocks in Figure 4 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.

The 5C design building blocks for I4.0 provides more narrowly focused concepts, but they lack the concrete action objectives that would enable the delivery of the ideas specified in Figure 4:3. The following layer of the I4.0 architecture model (Figure node 4:8) represents the 5C design actions for I4.0 with more concrete action objectives, such as; the development of AI reasoning, AI learning, and AI infrastructure in the case of NFIS initiative. This layer also includes (i) concrete funding sources, such as public funding, business contracts and collaborative projects; (ii) concrete goals to deliver, such as support sustainable business models; (iii) concrete actions, such as research collaboration; and concrete activities for feedback mechanisms, such as blog (forum). However, the design action stage of the I4.0

architecture models are still formulated by IVI and NTI deliberately in more general terms in order to provide flexibility in resolving each design action through different approaches present in the I4.0 initiatives around the world. For example, some of the 5C key projects for I4.0 identified, such as the HVM catapult, address part of the 5C design actions for I4.0 (e.g. the design element – Table 3). However, I4.0 involves more than the HVM catapult and, therefore, a new architecture model for national I4.0 strategy should integrate all the 11 catapults that form the UK I4.0 initiatives. In a similar process, the 5C key technologies for I4.0 layer should integrate all the 27 key technologies from the HVM catapult and all other UK I4.0 catapults.

The next layer of the proposed CPS-IoE-5C integration into I4.0 differs from most of the existing I4.0 initiatives. The 5C key tech sectors for I4.0 layer is based on the NTI guiding principle to focus on market creation as opposed to technology development. The argument of the Russian NTI initiative is that market development is the solution, rather than technology development. According to this initiative, in case there is a market for a specific technology, there will be the specific market mechanisms that will force development of the new technology. This approach seems to be compliant with the recent UK digital strategy, which promotes digital sectors and relates them to the wider economy, including data economy (DCMS, 2017). In this context, the 5C architecture for I4.0 aims to revolve the strategy around specific tech sectors. Therefore, the logical sequence in our architecture model is continued with the 5C key tech networks for I4.0 layer where technologies can be grouped to generate networks, similar to the NTI initiative (ASI, 2016). The new tech networks require 5C key testbeds for I4.0.

Global sharing of existing innovation testbeds (22 US testbeds from IIC; 11 UK catapults; over 500 projects in Germany), would reduce cost and enable faster product to marker process. Global sharing is also needed for the 5C industries and 5C key markets, bringing into focus the G20 initiative policy key point for trade liberalisation (G20, 2016). The second policy of the G20 initiative (the elimination of subsidies) is somewhat confusing. While there is a compiling argument for the elimination of subsidies in the traditional industries, the concept of CPS-IoE-5C-I4.0 integration requires technologies that are still in the infant stage of research and development. Economic policy dictates that infant industries need state support, hence emerging digital technologies also require state support. In any case, the NTI guiding principle (ASI, 2016) for focusing on market development is designed to reduce substantially any financial involvement of the state. The NTI (ASI, 2016) policy approach would address the second G20 policy key point 'the elimination of subsidies' (G20, 2016).

5. Discussion

This paper contributed with a new reference architecture model for the integration of the IIoT with existing processes from CPS and presented a design process for integrating these technologies in the I4.0. The reference architecture model is based on grouping of future and present techniques and presenting the design process through a new hierarchical framework and a new cascading model. These are established models for decomposing and reverse engineering design processes and in this paper, these models are applied following established engineering design methodologies. This results with a detailed step by step design process that can be applied by companies operating in this field, companies that are trying to evolve their operations, governments trying to improve their national strategies and governments trying to build national strategies. The contribution of the process developed in this study (outlined in Figure 4), for company practitioners is that they can easily check if their existing integration in the Industry 4.0, or companies that are trying to enter the I4.0, the findings of this study would enable them to build their digital strategies. The contributions of this study for national governments of the developed nations is that they can check and compare the existing digital strategies with the national digital strategies applied across the globe. The benefits for developing countries that have no digital strategies (e.g. most African, Latin American, Eastern European nations), is that they can review the current developments from around the world, and follow the step by step process to develop their national digital strategies for evolving in the Industry 4.0.

The methodologies applied in this study represent time-tested engineering design methods, such as the hierarchical framework and the cascading model combined with the grounded theory, which is a time-tested method for building new models. The validity of the new architecture model is validated through the inclusiveness of all existing frameworks from across the globe. This study reviewed all existing framework, starting from the world leading, less evolved and elusive frameworks related to the Industrial Internet of Things and Industry 4.0. In terms of CPS, the frameworks included in this study are selected based on the relevance to our topic, on the quality of the journal peer review and the number of citations. Considering the large number of frameworks and theories on CPSs, this was considered as the most reliable selection criteria for inclusion.

This resulted with a detailed and repetative process for creating a taxonomy of categories and grouping of concepts into integration design. The new design process was tested and versified with an empirical review of Industry 4.0 frameworks and results with a new step by step model for the integration of related systems and technologies (Industrial Internet of Things, Cyber Physical Systems, and Industry 4.0). We have seen that the systematic review of academic literature derived with a 5C architecture, challenges the established principles of a 6C architecture (GTAI, 2014; Industrie 4.0, 2017). The main argument of the emerging 5C architecture is that the community layer of the 6C architecture, is better represented as an SoS in the IoE because it represents multiple systems (not elements) working together towards a common goal (e.g. IoT, IoP and IoS). This represents a natural evolution of the integration of CPS-IoT-6C into I4.0 towards integration of the more encompassing CPS-IoE-5C into I4.0. The present and future techniques associated with the latter vision are outlined and represented in the I4.0 architecture model proposed in Table 4 and

Figure 4. Finally, the findings from academic literature are contrasted with a systematic review of 14 world leading I4.0 initiatives. The process of strategy cascading is applied with grounded theory to build an I4.0 architecture model that is grounded on academic knowledge and real-world practice.

The architectural model presented in this paper is designed to support the building of new I4.0 national strategies and the improving and reformulating of existing frameworks and practical initiatives. The architecture model would also benefit practitioners who aim to improve or evolve their operations in the I4.0 space. Similar model to the one presented in this paper does not exist in current literature - until present.

5.1 Validation of the I4.0 architecture model

In this paper, case studies of 14 world's leading I4.0 initiatives have been reviewed. Following the validation recommendations in other similar models (Toro, Barandiaran, and Posada, 2015), this paper proposed I4.0 reference architecture based upon the experiences from the empirical study of different ongoing world leading initiatives. Table 3 summarises the main elements of this study and indicates where individual aspects of the presented architecture are being implemented. However, research on CPS requires development of testbeds to validate the proposed solutions (Hahn et al., 2013). In scenarios where current testbeds have limited deployment capabilities for complex computation, the model design should be further validated through case studies (La and Kim, 2010).

5.2 Limitations and areas for further research

The architecture model for the integration of the CPS-IoE-5C into I4.0 requires further validation and delimiting, possibly through application to real world case studies. The process of implementing I4.0 is an evolutionary process, and as such, it would require flexibility in adapting the proposed framework to synchronise changes in the system complexities.

Alternative testing and validation of I4.0 architecture model

Some elements of CPS are still futuristic and require virtual validation in the design stages (Leitão, Colombo and Karnouskos, 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, Bauer, and Kuhn, 2015), unmanned network navigation (Wan et al., 2010), autonomous navigation (Berger and Rumpe, 2014), context aware CPS with Cloud Support (Wan et al., 2014a; Weyer et al., 2015), autonomous energy management (Wan et al., 2012) and integration of CPS in the cloud (Wan et al., 2014b). For validation, verification, optimisation and visualisation, advanced software tools can be applied (Pan et al., 2015). The next stage of development for the proposed I4.0 architecture model, is constituted by the application of these findings in multi-testbed / multi I4.0 initiatives settings. However, this process would require refining the findings and applying the reference architecture in a real-world setting,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 March 2019 doi:10.20944/preprints201903.0139.v1

which can take several years to complete.

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 as in Marwedel and Engel (2016). 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 (METI, 2015). Alternatively, industrial developers can test the 5C architecture by applying object oriented layered architecture for the cyber–physical components (Thramboulidis, 2015). However, to introduce performance measurements, the Thramboulidis (2015) 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.

This study proposed a new overarching I4.0 architecture model, and the holistic approach in this study can hardly be verified with the aforementioned methods. Nevertheless, these alternative approaches could be applied to validate individual components of the architecture model proposed.

Limitations in the economic and social areas

The article does not deal with the emerging literature on harnessing economic value from the I4.0 (Bauer, Hämmerle, Schlund and Vocke, 2015; Shafiq, Sanin, Szczerbicki, and Toro, 2015; Anderson, 2016; Brettel et al., 2016; Stock and Seliger, 2016; Wang et al., 2016; Hussain, 2017). Rather, the article points to the ways in which the reference architecture presented can inform the development of new economic models and future work on the actual assessment of emerging cyber risks in I4.0. This article is part of a series of articles published by this project and represents the preparation work for addressing the topic of harnessing economic value. Harnessing economic value is effectively a fundamental aspect of the approach particularly in relation to the economic risks that are briefly discussed in the paper. The focus of the article is on the integration of IIoT and I4.0 resulting with the reference architecture. Addressing all the related topics in a single article would have resulted with a lack of focus. Therefore, the authors had to consider what area the article is trying to address and focus it accordingly.

In addition, future research should give consideration of system sociology, because the conceptual grouping model presented does not address the question of skilled job losses (Dworschak and Zaiser, 2014). It is argued that technological unemployment is already happening in both routine and non-routine manufacturing tasks (e.g. Brynjolfsson and McAfee. 2011) and that the associated social disruptions will be significant as the technologically-driven labour market transitions are likely to take considerable time and domains such as in situations when AI accelerates the pace of automation (Kaplan, 2017). The counter argument is that skilled and educated jobs will be created to control and maintain machines (Dombrowski and Wagner, 2014) as I4.0 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 (Wahlster et al., 2013). We believe that elements in this article would also contribute to the ongoing debates on this topic.

The categorisation in Table 5 from a cyber security engineering perspective the 5C model in Section 5 is fundamentally flawed, referring to the middle layer as 'cyber' while cyber elements now extend from sensor/actuator through to supervisory control and advanced analytic solutions. The principles of grounded theory state that we need to report what we observe, not what we think its correct or incorrect. It is probably incorrect to use in this context, but it is used in this exact context in existing literature reviewed. Since the taxonomy is based on grounded theory, the fundamental principles of grounded theory are applied to categorise themes from existing literature. Once literature changes the wording, the wording of this category should change as well.

6. Conclusions

The complexities of the IIoT require a new regulatory framework and standardisation of a reference architecture for managing collaborative systems safely and securely while using resources efficiently. This paper presents a new model for the future vision for IIoT integration in a 5C-CPS architecture. The paper also identifies and provides a methodological design process for some specific grand challenges, such as cognition and AI in I4.0. The paper creates a taxonomy of common basic terminology, common approaches and existing world leading initiatives into a proposition of new economics architecture for I4.0. The paper also suggests the need to formulate compositional ways to reason about the emerging cyber risks in an I4.0 context. The proposed model enables the current efforts to integrate the IIoT into I4.0, and in a larger perspective the development of specific CPSs for I4.0.

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 IIoT in relation to I4.0. The paper combines approaches to incorporate existing standards into new design model for I4.0. Secondly, the paper captures some of the best practices in industry and develops a reference architecture using a step-by-step process design. This analysis includes reflection on how automation and AI could lower the cyber risk from the IIoT integration into the I4.0 future architectures. The paper presents the first I4.0 architecture model that integrates the recent academic literature on IIoT integration into I4.0 with the state-of-the-art practical initiatives that are currently at work in world's leading I4.0 initiatives.

7. References:

Ahmed, S.H., Kim, G. & Kim, D., 2013. Cyber Physical System: Architecture, applications and research challenges. In

2013 IFIP Wireless Days (WD). IEEE, pp. 1–5. Available at: http://ieeexplore.ieee.org/document/6686528/ [Accessed April 17, 2017].

Almeida, L., Santos, F. & Oliveira, L., 2016. Structuring Communications for Mobile Cyber-Physical Systems. In Springer International Publishing, pp. 51–76. Available at: http://link.springer.com/10.1007/978-3-319-26869-9_3 [Accessed April 15, 2017].

Anderson, G., 2016. The Economic Impact of Technology Infrastructure for Smart Manufacturing. *NIST Economic Analysis Briefs*, 4. Available at: http://nvlpubs.nist.gov/nistpubs/eab/NIST.EAB.4.pdf [Accessed April 4, 2017].

Anderson, R. & Moore, T., 2006. The Economics of Information Security. *Science*, 314(5799). Available at: http://science.sciencemag.org/content/314/5799/610.full [Accessed April 2, 2017].

Anon, 2013. AMP, Advanced Manufacturing Partnership. Available at: https://www.nist.gov/amo/programs [Accessed May 4, 2017].

Anon, 2013. *NIF, NEW INDUSTRIAL FRANCE*, Available at: https://www.economie.gouv.fr/files/files/PDF/web-dp-indus-ang.pdf [Accessed May 4, 2017].

Ashton, K., In the real world, things matter more than ideas. Available at: http://www.rfidjournal.com/articles/pdf?4986 [Accessed April 13, 2017].

ASI, A. for strategic initiatives, 2016. National Technology initiative, Agency for Strategic Initiatives. *Government of Russia*. Available at: https://asi.ru/eng/nti/ [Accessed May 10, 2017].

Balaji, B. et al., 2015. Models, abstractions, and architectures. In *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15*. New York, New York, USA: ACM Press, pp. 1–6. Available at: http://dl.acm.org/citation.cfm?doid=2744769.2747936 [Accessed April 17, 2017].

Bauer, W. et al., 2015. Transforming to a Hyper-connected Society and Economy – Towards an 'Industry 4.0.' *Procedia Manufacturing*, 3, pp.417–424. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2351978915002012 [Accessed April 18, 2017].

Benveniste, A., 2010. Loosely Time-Triggered Architectures for Cyber-Physical Systems. *2010 Design, Automation & Test in Europe Conference & Exhibition, Dresden*, pp.3–8.

Benveniste, A., Bouillard, A. & Caspi, P., 2010. A unifying view of loosely time-triggered architectures. In *Proceedings of the tenth ACM international conference on Embedded software - EMSOFT '10*. New York, New York, USA: ACM Press, p. 189. Available at: http://portal.acm.org/citation.cfm?doid=1879021.1879047 [Accessed April 26, 2017].

Berger, C. & Rumpe, B., 2014. Autonomous Driving - 5 Years after the Urban Challenge: The Anticipatory Vehicle as a Cyber-Physical System. Available at: http://arxiv.org/abs/1409.0413 [Accessed April 17, 2017].

Bhave, A. et al., 2010. Multi-domain Modeling of Cyber-Physical Systems Using Architectural Views. *Proceedings of the Analytic Virtual Integration of Cyber-Physical Systems Workshop*. Available at: http://repository.cmu.edu/isr/995 [Accessed April 17, 2017].

Bhave, A. et al., 2011. View Consistency in Architectures for Cyber-Physical Systems. In *2011 IEEE/ACM Second International Conference on Cyber-Physical Systems*. IEEE, pp. 151–160. Available at: http://ieeexplore.ieee.org/document/5945430/ [Accessed April 17, 2017].

Biener, C., Eling, M. & Wirfs, J.H., Insurability of Cyber Risk 1. Available at: https://www.genevaassociation.org/media/891047/ga2014-if14-biener_elingwirfs.pdf [Accessed April 3, 2017].

Bouws, T. et al., 2015. *Smart Industry: Dutch Industry Fit for the Future*, Delft. Available at: https://www.smartindustry.nl/site/assets/files/1744/opmaak-smart-industry.pdf [Accessed May 9, 2017].

Brettel, M. et al., 2016. Enablers for Self-optimizing Production Systems in the Context of Industrie 4.0. *Procedia CIRP*, 41, pp.93–98. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2212827115011440 [Accessed April 18, 2017].

Brynjolfsson, E. and McAfee, A. 2011. *Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy*. Lexington (MA): Digital Frontier Press.

Buith, J., 2016. *Cyber Value at Risk in the Netherlands*, Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf [Accessed April 4, 2017].

Carruthers, K., 2016. Internet of Things and Beyond: Cyber-Physical Systems - IEEE Internet of Things. *IEEE Internet of Things*. Available at: http://iot.ieee.org/newsletter/may-2016/internet-of-things-and-beyond-cyber-physical-systems.html [Accessed April 11, 2017].

Catapult, 2017. The Catapult Programme - Catapult. Available at: https://catapult.org.uk/ [Accessed May 13, 2017].

Cisco, 2013. The Internet of Everything Global Public Sector Economic Analysis. , pp.1–13. Available at: http://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysisfaq.pdf [Accessed July 3, 2017].

CoNSS, C. on N.S.S., 2010. *National Information Assurance (IA) Glossary*, Fort George G. Meade, MD.

Cook, G., 2012. *Greenpeace International: How Clean is Your Cloud?*, Amsterdam. Available at: http://www.greenpeace.org/international/Global/international/publications/climate/2012/iCoal/HowCleanisYourCloud.pdf [Accessed July 3, 2017].

Cook, Gary and Van Horn, J., 2011. *How Dirty is your Data? A Look at the Energy Choices that Power Cloud Computing*, Amsterdam. Available at: http://www.greenpeace.org/international/Global/international/publications/climate/2011/Cool IT/dirty-data-report-greenpeace.pdf [Accessed July 3, 2017].

DCMS, Department for Culture, Media and Sport, 2017. *UK Digital Strategy 2017 - GOV.UK*, London. Available at: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy [Accessed May 24, 2017].

Dillon, T.S. et al., 2011. Web-of-things framework for cyber-physical systems. *Concurrency and Computation: Practice and Experience*, 23(9), pp.905–923. Available at: http://doi.wiley.com/10.1002/cpe.1629 [Accessed April 17, 2017].

DiMase, D. et al., 2015. Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, 35(2), pp.291–300. Available at: http://dx.doi.org/10.1007/s10669-015-9540-y.

Dombrowski, U. & Wagner, T., 2014. Mental Strain as Field of Action in the 4th Industrial Revolution. *Procedia CIRP*, 17, pp.100–105. Available at: http://linkinghub.elsevier.com/retrieve/pii/S221282711400328X [Accessed April 18, 2017].

Drath, R. & Horch, A., 2014. Industrie 4.0: Hit or Hype? [Industry Forum]. *IEEE Industrial Electronics Magazine*, 8(2), pp.56–58. Available at: http://ieeexplore.ieee.org/document/6839101/ [Accessed April 18, 2017].

Dworschak, B. & Zaiser, H., 2014. Competences for Cyber-physical Systems in Manufacturing – First Findings and Scenarios. *Procedia CIRP*, 25, pp.345–350. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2212827114010798 [Accessed April 14, 2017].

Edgar, T. & Davis, J., 2015. *NSF Workshop on Research needs in Advanced Sensors, Controls, Platforms, and Modeling (ASCPM) for Smart Manufacturing*, Atlanta, Georgia. Available at: https://www.manufacturingusa.com/sites/all/assets/content/smlc_nsf_workshop_report.pdf [Accessed May 4, 2017].

Evans, P.C. & Annunziata, M., 2012. Industrial Internet: Pushing the Boundaries of Minds and Machines. Available at: https://www.ge.com/docs/chapters/Industrial_Internet.pdf [Accessed April 15, 2017].

Faller, C. & Feldmüller, D., 2015. Industry 4.0 Learning Factory for regional SMEs. *Procedia CIRP*, 32, pp.88–91. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2212827115001997 [Accessed April 18, 2017].

Feth, P., Bauer, T. & Kuhn, T., 2015. Virtual Validation of Cyber Physical Systems. *Software Engineering & Management*. Available at: http://cs.emis.de/LNI/Proceedings/Proceedings239/201.pdf [Accessed April 17, 2017].

G20, 2016. *G20 New Industrial Revolution Action Plan*, Available at: http://g20chn.org/English/Documents/Current/201609/P020160908738867573193.pdf [Accessed May 9, 2017].

Gershenfeld, N.A., 1999. *When things start to think*, Henry Holt. Available at: https://books.google.com/books?hl=en&lr=&id=J8GLAwAAQBAJ&oi=fnd&pg=PP2&dq=When+Things+Start+to+Think&ots=8HHfEEuYYh&sig=vSgqQS_0PtX0cH_E_d0uDVTYlCI#v=onepage&q=When Things Start to Think&f=false [Accessed April 13, 2017].

Giaimo, F. et al., 2016. Continuous Experimentation on Cyber-Physical Systems. In *Proceedings of the Scientific Workshop Proceedings of XP2016 on - XP '16 Workshops*. New York, New York, USA: ACM Press, pp. 1–2. Available at: http://dl.acm.org/citation.cfm?doid=2962695.2962709 [Accessed April 14, 2017].

Giordano, A., Spezzano, G. & Vinci, A., 2016. A Smart Platform for Large-Scale Cyber-Physical Systems. In Springer International Publishing, pp. 115–134. Available at: http://link.springer.com/10.1007/978-3-319-26869-9_6 [Accessed April 15, 2017].

Glaser, B.G. & Strauss, A.L., 1967. *The discovery of grounded theory : strategies for qualitative research*, Aldine Pub. Co.

Gordon, L.A. & Loeb, M.P., 2002. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), pp.438–457. Available at: http://portal.acm.org/citation.cfm?doid=581271.581274 [Accessed April 2, 2017].

GTAI, G.T. and I., 2014. *Industrie 4.0 Smart Manufacturing for the Future*, Berlin. Available at: https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future-en.pdf [Accessed May 9, 2017].

Gubbi, J. et al., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future*

Generation Computer Systems, 29(7), pp.1645–1660. Available at: http://www.sciencedirect.com/science/article/pii/S0167739X13000241 [Accessed August 11, 2016].

Guerrieri, A. et al., 2016. *Management of cyber physical objects in the future internet of things : methods, architectures and applications*,

Hahn, A. et al., 2013. Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. *IEEE Transactions on Smart Grid*, 4(2), pp.847–855. Available at: http://ieeexplore.ieee.org/document/6473865/ [Accessed April 17, 2017].

Hamilton, B.A., 2014. Cyber Power Index. , pp.1–36. Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU - Cyber Power Index Findings and Methodology.pdf [Accessed April 3, 2017].

Hermann, M., Pentek, T. & Otto, B., 2016. Design Principles for Industrie 4.0 Scenarios. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, pp. 3928–3937. Available at: http://ieeexplore.ieee.org/document/7427673/ [Accessed April 18, 2017].

Hussain, F., 2017. Internet of Everything. In *Internet of Things: Building Blocks and Business Models*. Springer International Publishing, pp. 1–11. Available at: http://link.springer.com/10.1007/978-3-319-55405-1_1 [Accessed April 20, 2017].

Huth, M, Vishik, C., and Masucci, R. 2016. 'From Risk Management to Risk Engineering: Challenges in Future ICT Systems.' In Griffor, E., ed., *Handbook of System Safety and Security*, p. 131-174.

IIC, I.I.C., 2017. *The Industrial Internet of Things Volume G5: Connectivity Framework*, Available at: http://www.iiconsortium.org/pdf/IIC_PUB_G5_V1.0_PB_20170228.pdf [Accessed May 4, 2017].

Industrie 4.0, 2017. Plattform Industrie 4.0 - Testbeds. Available at: http://www.plattform-i40.de/I40/Navigation/EN/InPractice/Testbeds/testbeds.html [Accessed May 13, 2017].

IVI, I.V.C.I., 2017. *Industrial Value Chain Reference Architecture*, Hannover, Germany. Available at: https://iv-i.org/en/docs/Industrial_Value_Chain_Reference_Architecture_170424.pdf [Accessed May 4, 2017].

IVI. Industrial Value Chain Initiative, 2016. An Outline of Smart Manufacturing Scenarios 2016. In *Monozukuri Nippon Conference*. Tokyo. Available at: https://iv-i.org/en/docs/ScenarioWG_2016.pdf [Accessed May 4, 2017].

Jazdi, N., 2014. Cyber physical systems in the context of Industry 4.0. In *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*. IEEE, pp. 1–4. Available at: http://ieeexplore.ieee.org/document/6857843/ [Accessed April 14, 2017].

Jensen, J.C., Chang, D.H. & Lee, E.A., 2011. A model-based design methodology for cyber-physical systems. In *2011 7th International Wireless Communications and Mobile Computing Conference*. IEEE, pp. 1666–1671. Available at: http://ieeexplore.ieee.org/document/5982785/ [Accessed April 17, 2017].

John, P., 2017. *High Value Manufacturing Catapult*, Solihull. Available at: https://ec.europa.eu/growth/tools-databases/regional-innovation-monitor/sites/default/files/report/High Value Manufacturing Catapult_1.pdf [Accessed May 9, 2017].

Kambatla, K. et al., 2014. Trends in big data analytics. *J. Parallel Distrib. Comput*, 74, pp.2561–2573. Available at: www.elsevier.com/locate/jpdc [Accessed April 11, 2017].

Kang, W., Kapitanova, K. & Son, S.H., 2012. RDDS: A Real-Time Data Distribution Service for Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics*, 8(2), pp.393–405. Available at: http://ieeexplore.ieee.org/document/6129422/ [Accessed April 17, 2017].

Kaplan, J. 2017. 'Artificial Intelligence: Think Again.' In *Communications of the ACM*, 60(1): 36-38.

Kirkpatrick, K., 2013. Software-defined networking. *Communications of the ACM*, 56(9), p.16. Available at: http://dl.acm.org/citation.cfm?doid=2500468.2500473 [Accessed April 11, 2017].

Koch, R. & Rodosek, G., *Proceedings of the 15th European Conference on Cyber Warfare and Security : ECCWS 2016 : hosted by Universität der Bundeswehr, Munich, Germany 7-8 July 2016*, Available at: https://books.google.co.uk/books?hl=en&lr=&id=ijaeDAAAQBAJ&oi=fnd&pg=PA145&dq=economic+impact+of+cyber+risk&ots=50mTo8TVSV&sig=sD4V76yG5tG6IZlglmnGz3L1qqw&redir_esc=y#v=onepage&q=economic impact of cyber risk&f=false [Accessed April 3, 2017].

Kolberg, D. & Zühlke, D., 2015. Lean Automation enabled by Industry 4.0 Technologies. *IFAC-PapersOnLine*, 48(3), pp.1870–1875. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2405896315005984 [Accessed April 18, 2017].

Kumar, P. et al., 2012. A hybrid approach to cyber-physical systems verification. In *Proceedings of the 49th Annual Design Automation Conference on - DAC '12*. New York, New York, USA: ACM Press, pp. 688–696. Available at: http://dl.acm.org/citation.cfm?doid=2228360.2228484 [Accessed April 17, 2017].

La, H.J. & Kim, S.D., 2010. A Service-Based Approach to Designing Cyber Physical Systems. In *2010 IEEE/ACIS 9th International Conference on Computer and Information Science*. IEEE, pp. 895–900. Available at: http://ieeexplore.ieee.org/document/5591233/ [Accessed April 17, 2017].

Lee, J., Bagheri, B. & Kao, H.A., 2015. *A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems*, Available at: http://www.sciencedirect.com/science/article/pii/S221384631400025X [Accessed April 14, 2017].

Lee, J., Kao, H.-A. & Yang, S., 2014. Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment. *Procedia CIRP*, 16, pp.3–8. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2212827114000857 [Accessed April 18, 2017].

Leitão, P., Colombo, A.W. & Karnouskos, S., 2016. Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Computers in Industry*, 81, pp.11–25. Available at: http://www.sciencedirect.com/science/article/pii/S0166361515300348 [Accessed April 15, 2017].

Lewis, D. & Brigder, D., 2004. Market Researchers make Increasing use of Brain Imaging. *Advances in clinical neuroscience and rehabilitation*, 5(3), pp.36–37. Available at: http://www.acnr.co.uk/pdfs/volume5issue3/v5i3specfeat.pdf [Accessed April 11, 2017].

Longstaff, T.A. & Haimes, Y.Y., 2002. A holistic roadmap for survivable infrastructure systems. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 32(2), pp.260–268. Available at: http://ieeexplore.ieee.org/document/1021113/ [Accessed April 11, 2017].

Madakam, S., Ramaswamy, R. & Tripathi, S., 2015. Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, 3(3), pp.164–173. Available at: http://www.scirp.org/journal/jcc [Accessed April 13, 2017].

Marwedel, P. & Engel, M., 2016. Cyber-Physical Systems: Opportunities, Challenges and (Some) Solutions. In Springer International Publishing, pp. 1–30. Available at: http://link.springer.com/10.1007/978-3-319-26869-9_1 [Accessed April 15, 2017].

MEICA, M. of E.I. and C.A., 2015. *Industria Conectada 4.0: La transformación digital de la industria española Dossier de prensa*, Madrid. Available at: http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/081015 Dossier prensa Industria 4 0.pdf [Accessed May 9, 2017].

METI, M. of E.T. and I. of J., 2015. *NRS, New Robot Strategy - Vision Strategy and Action Plan*, Available at: http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf [Accessed July 3, 2017].

METI, M. of E.T. and I. of J., 2015. *NRS, New Robot Strategy - Vision Strategy and Action Plan*, Available at: http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf [Accessed July 3, 2017].

MIUR, M. of E.U. and R., 2014. Italian Technology Cluster: Intelligent Factories. *Cluster Tecnologico Nazionale Fabbrica Intelligente | Imprese, università, organismi di ricerca, associazioni e enti territoriali: insieme per la crescita del Manifatturiero*. Available at: http://www.fabbricaintelligente.it/en/ [Accessed May 9, 2017].

Nicolescu, R. et al., 2018a. Mapping the values of IoT. Journal of Information Technology, pp.1–16. Available at: http://link.springer.com/10.1057/s41265-018-0054-1 [Accessed March 27, 2018].

Nicolescu, R. et al., 2018b. State of The Art in IoT - Beyond Economic Value, London. Available at: https://iotuk.org.uk/wp-content/uploads/2018/08/State-of-the-Art-in-IoT-—-Beyond-Economic-Value2.pdf [Accessed October 14, 2018].

Niggemann, O. et al., 2015. 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)*. Available at: http://ceur-ws.org/Vol-1507/dx15paper24.pdf [Accessed April 15, 2017].

NIST, National Institute of Standards and Technology, 2016. *Framework for Cyber-Physical Systems*. Release 1.0. Available at: https://pages.nist.gov/cpspwg/ {Accessed 15 June, 2017].

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

Nurse, J.R.C. et al., 2018. 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. 28 - 29 March 2018 | IET London: Savoy Place: The Institution of Engineering and Technology, pp. 1–9. Available at: https://ieeexplore.ieee.org/document/8379688/ [Accessed June 1, 2018].

Olzak, T., 2013. Insider threats: Implementing the right controls - TechRepublic. *TechRepublic*. Available at: http://www.techrepublic.com/blog/it-security/insider-threats-implementing-the-right-controls/ [Accessed April 10, 2017].

Ouyang, J. et al., 2014. SDF. In *Proceedings of the 19th international conference on Architectural support for programming languages and operating systems - ASPLOS ’14*. New York, New York, USA: ACM Press, pp. 471–484. Available at: http://dl.acm.org/citation.cfm?doid=2541940.2541959 [Accessed April 11, 2017].

Pan, M. et al., 2015. Applying Industry 4.0 to the Jurong Island Eco-industrial Park. *Energy Procedia*, 75, pp.1536–

1541. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1876610215010814 [Accessed April 18, 2017].

Petrolo, R., Loscri, V. & Mitton, N., 2016. Cyber-Physical Objects as Key Elements for a Smart Cyber-City. In Springer International Publishing, pp. 31–49. Available at: http://link.springer.com/10.1007/978-3-319-26869-9_2 [Accessed April 15, 2017].

Posada, J. et al., 2015. Visual Computing as a Key Enabling Technology for Industrie 4.0 and Industrial Internet. *IEEE Computer Graphics and Applications*, 35(2), pp.26–40. Available at: http://ieeexplore.ieee.org/document/7064655/ [Accessed April 18, 2017].

Radanliev, P. (2014) 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. doi: ISNI: 0000 0004 5352 6866.

Radanliev, P. (2015a) 'Architectures for Green-Field Supply Chain Integration', Journal of Supply Chain and Operations Management. GB, 13(2). Available at: https://www.csupom.com/uploads/1/1/4/8/114895679/2015n5p5.pdf (Accessed: 11 August 2016).

Radanliev, P. (2015b) 'Engineering Design Methodology for Green-Field Supply Chain Architectures Taxonomic Scheme', Journal of Operations and Supply Chain Management. GB, 8(2), pp. 52–66. doi: 10.12660/joscmv8n2p52-66.

Radanliev, P. (2015c) 'Green-field Architecture for Sustainable Supply Chain Strategy Formulation', International Journal of Supply Chain Management. GB, 4(2), pp. 62–67. Available at: http://ojs.excelingtech.co.uk/index.php/IJSCM/article/view/1060/pdf (Accessed: 11 August 2016).

Radanliev, P. (2016) 'Supply Chain Systems Architecture and Engineering Design: Green-field Supply Chain Integration', Operations and Supply Chain Management: An International Journal, 9(1). Available at: http://www.journal.oscm-forum.org/journal/abstract/oscm-volume-9-issue-1-2016/supply-chain-systems-architecture-and-engineering-design-green-field-supply-chain-integration (Accessed: 21 July 2017).

Radanliev, P., Charles De Roure, D., Maple, C., Nurse, J. R. C., Nicolescu, R. and Ani, U. (2019a) Cyber Risk in IoT Systems, Journal of Cyber Policy. University of Oxford. doi: 10.13140/RG.2.2.29652.86404.

Radanliev, P., Charles De Roure, D., Nurse, J. R. C., Burnap, P. and Montalvo, R. M. (2019) Methodology for designing decision support supply chain systems for visualising and mitigating cyber risk from IoT technologies, Working paper. University of Oxford. doi: 10.13140/RG.2.2.32975.53921.

Radanliev, P., De Roure, C. D., Nurse, .R.C., Nicolescu, R., Huth, M., Cannady, C. and Montalvo, R. M. (2018) '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. London: IET, p. 41 (6 pp.)-41 (6 pp.). doi: 10.1049/cp.2018.0041.

Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., Maddox, L., Santos, O. and Montalvo, R. M. (2019b) Cyber risk from IoT technologies in the supply chain – decision support system for the Industry 4.0. University of Oxford.

Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., Maddox, L., Santos, O. and Montalvo, R. M. (2019c) Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment. 201903.0080.v1. Oxford: Preprints. doi: 10.13140/RG.2.2.17305.88167.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., Santos, O. and Montalvo, R. M. (2019d) 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, Working paper. University of Oxford.

Radanliev, P., De Roure, D. C., Nurse, J. R. C. C., Nicolescu, R., Huth, M., Cannady, S. and Montalvo, R. M. (2019e) 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. doi: 10.13140/RG.2.2.14133.93921.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M. and Burnap, P. (2019f) Standardisation of cyber risk impact assessment for the Internet of Things (IoT). University of Oxford.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M. and Burnap, P. (2019g) The Industrial Internet-of-Things in the Industry 4.0 supply chains of small and medium sized enterprises, Working paper. University of Oxford.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M., Burnap, P., Roure, D. C. De, Nurse, J. R. C., Montalvo, R. M. and Stacy Cannady (2019h) Design principles for cyber risk impact assessment from Internet of Things (IoT), Working paper. University of Oxford.

Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Montalvo, R. M. and Stacy Cannady (2018) 'Design principles for cyber risk impact assessment from Internet of Things (IoT)', Wokring paper.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Rafael, M. M. and Burnap, P. (2019i) Supply Chain Design for the Industrial Internet of Things and the Industry 4.0. University of Oxford. doi: 10.13140/RG.2.2.36311.32160.

Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R. and Huth, M. (2018) '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. London: Institution of Engineering and Technology, p. 3 (9 pp.)-3 (9 pp.). doi: 10.1049/cp.2018.0003.

Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R. and Huth, M. (2019j) Analysing IoT cyber risk for estimating IoT cyber insurance. Available at: www.preprints.org.

Radanliev, P., De Roure, D., Nicolescu, R. and Huth, M. (2019k) A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0, Working paper. University of Oxford.

Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S. and Burnap, P. (2018) 'Future developments in cyber risk assessment for the internet of things', Computers in Industry. Elsevier, 102, pp. 14–22. doi: 10.1016/J.COMPIND.2018.08.002.

Radanliev, P., De Roure, D., Nurse, J. R. C. C., Nicolescu, R., Huth, M., Cannady, S. and Montalvo, R. M. (2019l) Cyber risk impact assessment – assessing the risk from the IoT to the digital economy. University of Oxford. doi: 10.13140/RG.2.2.11145.49768.

Radanliev, P., De Roure, D., Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S. and Montalvo, R. M. (2019m) Cyber Security Framework for the Internet-of-Things in Industry 4.0. Available at: www.preprints.org.

Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L., Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, H., Cooper, R., Coulton, P., Craggs, B.,Davies, N., De Roure, D., Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, B., Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, A., Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, R., Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., T. and R.J., Westbury, P. S. (2018) Internet of Things realising the potential of a trusted smart world. London. Available at: www.raeng.org.uk/internetofthings (Accessed: 31 March 2018).

Rajkumar, R. (Raj), Lee, I., Sha, L., & Stankovic, J. 2010. Cyber-Physical Systems: The Next Computing Revolution. In *Proceedings of the 47th Design Automation Conference on - DAC '10*. New York, New York, USA: ACM Press, p. 731. Available at: https://www.cs.virginia.edu/~stankovic/psfiles/Rajkumar-DAC2010-Final.pdf [Accessed April 11, 2017].

Ribeiro, L., Barata, J. & Ferreira, J., 2010. An agent-based interaction-oriented shop floor to support emergent diagnosis. In *2010 8th IEEE International Conference on Industrial Informatics*. IEEE, pp. 189–194. Available at: http://ieeexplore.ieee.org/document/5549436/ [Accessed April 15, 2017].

Ringert, J.O., Rumpe, B. & Wortmann, A., 2014. From Software Architecture Structure and Behavior Modeling to Implementations of Cyber-Physical Systems. Available at: http://arxiv.org/abs/1408.5690 [Accessed April 17, 2017].

Ringert, J.O., Rumpe, B. & Wortmann, A., 2015. Architecture and Behavior Modeling of Cyber-Physical Systems with MontiArcAutomaton. Available at: http://arxiv.org/abs/1509.04505 [Accessed April 17, 2017].

Rodewald, G. & Gus, 2005. Aligning information security investments with a firm's risk tolerance. In *Proceedings of the 2nd annual conference on Information security curriculum development - InfoSecCD '05*. New York, New York, USA: ACM Press, p. 139. Available at: http://portal.acm.org/citation.cfm?doid=1107622.1107654 [Accessed April 2, 2017].

Roumani, M.A. et al., 2016. Value Analysis of Cyber Security Based on Attack Types. *ITMSOC Transactions on Innovation & Business Engineering*, 1, pp.34–39. Available at: http://www.itmsoc.org [Accessed April 4, 2017].

Ruan, K., 2017. Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, 65, pp.77–89. Available at: http://www.sciencedirect.com/science/article/pii/S0167404816301407 [Accessed April 2, 2017].

Ruffle, S.J.; Bowman, G.; Caccioli, F.; Coburn, A.W.; Kelly, S.; Leslie, B.; Ralph, D., 2014. Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe. *Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.* Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/ccrs_cyber_catastrophe_scenario_october_2014.pdf [Accessed April 4, 2017].

Sirris and Agoria, 2017. Made Different: Factory of the Future 4.0. Available at: http://www.madedifferent.be/en/what-factory-future-40 [Accessed May 9, 2017].

Sangiovanni-Vincentelli, A., Damm, W. & Passerone, R., 2012. Taming Dr. Frankenstein: Contract-Based Design for Cyber-Physical Systems * g. *European Journal of Control*, 18, pp.217–238. Available at: http://ac.els-cdn.com/S0947358012709433/1-s2.0-S0947358012709433-main.pdf?_tid=83e4d7ce-22f9-11e7-860b-00000aacb362&acdnat=1492384251_7a3da72078e34a158bde90e76bb87fee [Accessed April 17, 2017].

SCPRC, T.S.C.P.R. of C., 2017. Made in China 2025. *www.english.gov.cn*. Available at: http://english.gov.cn/2016special/madeinchina2025/ [Accessed May 10, 2017].

Shackelford, S.J., 2016. Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk. *Chapman Law Review*, 19. Available at: http://heinonline.org/HOL/Page?handle=hein.journals/chlr19&id=469&div=26&collection=journals [Accessed April 3, 2017].

Shafiq, S.I. et al., 2015. Virtual Engineering Object / Virtual Engineering Process: A specialized form of Cyber Physical System for Industrie 4.0. *Procedia Computer Science*, 60, pp.1146–1155. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1877050915022930 [Accessed April 18, 2017].

Shi, J. et al., 2011. A survey of Cyber-Physical Systems. In *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, pp. 1–6. Available at: http://ieeexplore.ieee.org/document/6096958/ [Accessed April 17, 2017].

Sokolov, B. & Ivanov, D., 2015. Integrated scheduling of material flows and information services in industry 4.0 supply networks. *IFAC-PapersOnLine*, 48(3), pp.1533–1538. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2405896315005431 [Accessed April 18, 2017].

Stock, T. & Seliger, G., 2016. Opportunities of Sustainable Manufacturing in Industry 4.0. *Procedia CIRP*, 40, pp.536–541. Available at: http://linkinghub.elsevier.com/retrieve/pii/S221282711600144X [Accessed April 18, 2017].

Stojmenovic, I., 2014. Machine-to-Machine Communications With In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems. *IEEE Internet of Things Journal*, 1(2), pp.122–128. Available at: http://ieeexplore.ieee.org/document/6766661/ [Accessed April 17, 2017].

Taylor, L., 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.

Tan, Y., Goddard, S. & Pérez, L.C., 2008. A Prototype Architecture for Cyber-Physical Systems. *ACM SIGBED Review - Special issue on the RTSS forum on deeply embedded real-time computing*, 5(1). Available at: http://delivery.acm.org/10.1145/1370000/1366309/p26-tan.pdf?ip=129.67.116.155&id=1366309&acc=ACTIVE SERVICE&key=BF07A2EE685417C5.F2FAECDC86A918EB.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=922793771&CFTOKEN=47199625&__acm__=1492383641_ca27b2c456d59140 [Accessed April 16, 2017].

Thramboulidis, K., 2015. A cyber–physical system-based approach for industrial automation systems. *Computers in Industry*, 72, pp.92–102. Available at: http://www.sciencedirect.com/science/article/pii/S0166361515000962 [Accessed April 14, 2017].

Toro, C., Barandiaran, I. & Posada, J., 2015. A Perspective on Knowledge Based and Intelligent Systems Implementation in Industrie 4.0. *Procedia Computer Science*, 60, pp.362–370. Available at: http://linkinghub.elsevier.com/retrieve/pii/S187705091502270X [Accessed April 18, 2017].

USDA, U.S.D. of A., 2001. *Field manual physical security*, Washington.

Wahlster, W. et al., 2013. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*, Available at: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf [Accessed April 14, 2017].

Wan, J. et al., 2011. A General Test Platform for Cyber-Physical Systems: Unmanned Vehicle with Wireless Sensor Network Navigation. *Procedia Engineering*, 24, pp.123–127. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1877705811054658 [Accessed April 17, 2017].

Wan, J. et al., 2013. Cyber-Physical Systems for Optimal Energy Management Scheme of Autonomous Electric Vehicle. *The Computer Journal*, 56(8), pp.947–956. Available at: https://academic.oup.com/comjnl/article-lookup/doi/10.1093/comjnl/bxt043 [Accessed April 17, 2017].

Wan, J. et al., 2013. From machine-to-machine communications towards cyber-physical systems. *Computer Science and Information Systems*, 10(3), pp.1105–1128. Available at: http://www.doiserbia.nb.rs/Article.aspx?ID=1820-02141300018W [Accessed April 17, 2017].

Wan, J. et al., 2014. Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions. *IEEE Communications Magazine*, 52(8), pp.106–113. Available at: http://ieeexplore.ieee.org/document/6871677/ [Accessed April 16, 2017].

Wan, J. et al., 2014. VCMIA: A Novel Architecture for Integrating Vehicular Cyber-Physical Systems and Mobile Cloud Computing. *Mobile Networks and Applications*, 19(2), pp.153–160. Available at: http://link.springer.com/10.1007/s11036-014-0499-6 [Accessed April 17, 2017].

Wan, J., Cai, H. & Zhou, K., 2015. Industrie 4.0: Enabling technologies. In *Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things*. IEEE, pp. 135–140. Available at: http://ieeexplore.ieee.org/document/7111555/ [Accessed April 18, 2017].

Wang, L. et al., 2014. A cloud-based approach for WEEE remanufacturing. *CIRP Annals - Manufacturing Technology*, 63(1), pp.409–412. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0007850614001176 [Accessed April 15, 2017].

Wang, L., 2013. Machine availability monitoring and machining process planning towards Cloud manufacturing. *CIRP Journal of Manufacturing Science and Technology*, 6(4), pp.263–273. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1755581713000527 [Accessed April 15, 2017].

Wang, L., Törngren, M. & Onori, M., 2015. Current status and advancement of cyber-physical systems in manufacturing. *Journal of Manufacturing Systems*, 37, pp.517–527. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0278612515000400 [Accessed April 15, 2017].

Wang, S. et al., 2016. Implementing Smart Factory of Industrie 4.0: An Outlook. *International Journal of Distributed Sensor Networks*, 12(1), p.3159805. Available at: http://journals.sagepub.com/doi/10.1155/2016/3159805 [Accessed April 18, 2017].

Wark, T. et al., 2007. Transforming Agriculture through Pervasive Wireless Sensor Networks. *IEEE Pervasive Computing*, 6(2), pp.50–57. Available at: http://ieeexplore.ieee.org/document/4160605/ [Accessed April 11, 2017].

Weyer, S. et al., 2015. Towards Industry 4.0 - Standardization as the crucial challenge for highly modular, multi-vendor production systems. *IFAC-PapersOnLine*, 48(3), pp.579–584. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2405896315003821 [Accessed April 18, 2017].

Zhu, Q., Rieger, C. & Basar, T., 2011. A hierarchical security architecture for cyber-physical systems. In *2011 4th International Symposium on Resilient Control Systems*. IEEE, pp. 15–20. Available at:

 doi:10.20944/preprints201903.0139.v1

http://ieeexplore.ieee.org/document/6016081/ [Accessed April 17, 2017].