Research Article

Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge

Petar Radanliev[1] · David De Roure[1] · Rob Walton[1] · Max Van Kleek[2] · Rafael Mantilla Montalvo[3] · La'Treall Maddox[3] · Omar Santos[3] · Peter Burnap[4] · Eirini Anthi[4]

Received: 22 April 2020 / Accepted: 21 September 2020 / Published online: 6 October 2020

Abstract
We explore the potential and practical challenges in the use of artificial intelligence (AI) in cyber risk analytics, for improving organisational resilience and understanding cyber risk. The research is focused on identifying the role of AI in connected devices such as Internet of Things (IoT) devices. Through literature review, we identify wide ranging and creative methodologies for cyber analytics and explore the risks of deliberately influencing or disrupting behaviours to socio-technical systems. This resulted in the modelling of the connections and interdependencies between a system's edge components to both external and internal services and systems. We focus on proposals for models, infrastructures and frameworks of IoT systems found in both business reports and technical papers. We analyse this juxtaposition of related systems and technologies, in academic and industry papers published in the past 10 years. Then, we report the results of a qualitative empirical study that correlates the academic literature with key technological advances in connected devices. The work is based on grouping future and present techniques and presenting the results through a new conceptual framework. With the application of social science's grounded theory, the framework details a new process for a prototype of AI-enabled dynamic cyber risk analytics at the edge.

Keywords Artificial cognition · Internet of things · Cyber-physical systems · Artificial intelligence · Machine learning · Automatic anomaly detection system · Dynamic analytics

1 Introduction

It has been argued that the spectacular advancements in cyber-physical systems (CPSs) and Internet of things (IoT) technology represent the foundation for Industry 4.0 [1], an IoT term originated in 1999 [2], along with the first view of how an IoT-based environment might look like in the future [3]. The term CPS encompasses the complex and multidisciplinary aspects of 'smart' systems that are built and depend on the interaction between physical and computational components [4]. CPS theory emerged from control theory and control systems engineering and focuses on the interconnection of physical components and use of complex software entities to establish new network and systems capabilities. CPSs thus link physical and engineered systems and bridge the cyber world with the physical world.

In contrast, IoT theory emerged from computer science and Internet technologies and focuses mainly on the interconnectivity, interoperability and integration of physical components on the Internet. With full IoT market adoption over the next decade, this integration work is anticipated to lead to developments such as IoT automation of CPSs [5,

✉ Petar Radanliev, petar.radanliev@oerc.ox.ac.uk | [1]Engineering Science Department, Oxford E-Research Centre, University of Oxford, 7 Keble Road, Oxford OX1 3QG, England, UK. [2]Department of Computer Science, University of Oxford, Oxford, England, UK. [3]Cisco Research Centre, Research Triangle Park, Durham, North Carolina, USA. [4]School of Computer Science and Informatics, Cardiff University, Cardiff, Wales, UK.

6], real-time enabled CPS platforms and automated CPSs that guide skilled workers in production environments [7].

In this context, we investigate how such systems enable artificial intelligence (AI) advances in real-time processing, sensing and actuation between these new systems and provide capabilities for system analysis of the cyber structures involved [8]. We therefore focus here on artificial intelligence, representing a concept that consolidates the cyber-physical and social aspects of the risks in which new technology is deployed [9].

The objective of this study was to build upon existing work on cyber risk standardisation [10], and AI in CPS [11], but with a greater focus on exploring the potential and practical challenges in the use of AI, in the service of improving personal and organisational resilience. The methodology applied in the study follows recommendations in existing studies on adaptive risk models [12]; feedback in IoT systems [13]; in layered IoT architecture [14]; and for optimising decision-making [15]. We identified approaches to model the risk within complex interconnected and coupled systems in cyber-physical environments. This involved modelling the connections and interdependencies between components to both external and internal services and systems. In modelling the connections and interdependencies, we studied CPSs that demonstrate the use and application of IoT technology.

The research reported here has two research objectives. Firstly, we present an up to date overview of existing and emerging advancements in the field of cyber risk analytics. This combines the existing literature to derive common basic terminology and approaches and to incorporate existing standards into a new feedback mechanism for risk analytics. Secondly, we capture the best practices and provoke a debate among practitioners and academics by offering a new understanding of network cyber risk and the role of AI in future CPS. This architecture is developed throughout the paper and can serve as a best practice and inform initial steps taken for design and prototype of AI-enabled dynamic cyber risk analytics.

2 Literature review on artificial intelligence, CPS and predictive cyber risk analytics

CPSs and IoT produce a vast amount of data, and the analysis of such big data requires advanced analytical tools. For clearing up the noise and inconsistency of the data, we almost certainly require AI-enhanced analytical tools [16]. In terms of data streams, the IoT has been described as a revolutionary technology enhancement that changes traditional life into a high tech lifestyle [17]. CPS architectures on the other hand represent a very broad concept [18]. A system must integrate these diverse concepts into a cognitive state for big data analytics and statistical machine learning to predict cyber risks [19]. But the design of big data systems for edge computing environments is challenging [20].

One of the most pressing points for CPS is perhaps security [21], both electronic and physical, that relates physical and cyber systems [22]. Such security requires information assurance and protection for data in transit from physical and electronic domains and storage facilities [23]. In addition, asset management and access control are required for granting or denying requests to information and processing services [24], especially because CPS will interface with nontechnical users and because influence across administrative boundaries is possible [25]. Techniques are needed to address novel vulnerabilities caused by life cycle issues including diminishing manufacturing sources and the update of assets [26]. These include approaches for engineering system dynamics across multiple timescales [27], like loosely time-triggered architectures [28] and structure dynamics control [29].

Furthermore, CPS requires anti-counterfeit and supply chain risk management to counteract malicious supply chain components that have been modified from their original design to cause disruption or unauthorised function [30]. Along with standardisation of design and process [31], hyper-connectivity in the digital supply chain [32] also needs to be supported. It is suggested that limiting source code access to crucial and skilled personnel can provide software assurance and application security and may be necessary for eliminating the introduction of deliberate flaws and vulnerabilities in CPSs [33].

Security measures should include forensics, prognostics and recovery plans, for the analysis of cyber-attacks and for co-ordination with other CPSs and entities that identify external cyber-attack vectors. To address this, an internal track and trace network process can assist in detecting or preventing the existence of weaknesses in the logistics security controls [34]. To support this, a process for anti-malicious and anti-tamper system engineering is needed to prevent the exploitation of CPS vulnerabilities identified through reverse engineering attacks [35].

2.1 Taxonomy of focus areas for artificial intelligence for CPS risk analytics

The Smart literature review framework based on latent Dirichlet allocation [36] was used to perform a taxonomic analysis. The resulting areas of focus are presented in a taxonomy with abbreviations (Table 1) that support the robust integration of artificial intelligence with existing CPS architecture systems [37]. The taxonomy presents the areas of focus identified in the literature on cyber risk

Table 1 Taxonomy of areas of focus (AoF) for cognitive feedback mechanism in predictive cyber risk analytics

Taxonomy of focus areas for artificial intelligence for CPS risk analytics—Glossary of acronyms 2	
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

analytics [38], where cyber and physical components and connectors constitute the entire system at runtime [39].

The areas of focus (AoF) in Table 1 emphasise the need for privacy in the feedback mechanism for cyber-attack reporting and shared databases in CPS risk analytics. In the following section, systematic analysis is applied to each focal area to determine its overlap with the literature on artificial intelligence in CPS predictive cyber risk analytics.

3 Artificial intelligence for manufacturing and 'servitization'

'Servitization' is a move from selling physical products to selling the ongoing services that those products perform or the ongoing services that support a products' operation. In the context of artificial intelligence in CPS risk analytics these services include predictive maintenance, the forecasting of machine failure and the automatic diagnosis of failures. For example, intelligent machine-learning algorithms take information from industrial IoT sensors and platforms in order to automatically diagnose failures and estimate the remaining useful life of machinery.

3.1 Grounded theory for taxonomies design

Here, we are applying the grounded theory (GT) method to group the requirements for artificial intelligence for CPS risk analytics for 'servitization' in manufacturing. The grounded theory analysis is built into a conceptual diagram in Fig. 1, representing the cascading hierarchical process through the areas of focus for CPS security.

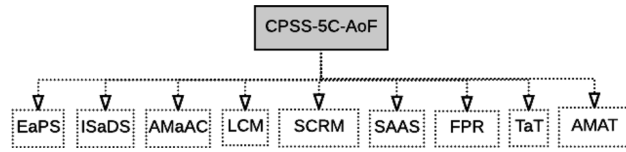

Fig. 1 CPS security in the areas of focus in five levels of CPSs

Figure 1 is a tool for visualising the areas of focus derived from the analysis. The areas of focus in Fig. 1 are latter classified in the five levels of artificial intelligence in CPS (see Table 3).

3.1.1 Electronic and physical security for artificial technologies—EaPS

This requires real-time data acquisition and storage solutions [40] for fleets of machines [41], providing adaptive analysis and peer-to-peer monitoring.

3.1.2 Information assurance and data security for artificial technologies—ISaDS

This needs to be supported with autonomous cognitive decisions, machine-learning algorithms and high-performance computing or data analysis [42], supported with fast cyber-attack information sharing and reporting via shared database resources.

3.1.3 Asset management and access control for cyber risk analytics—AMaAC

In dynamic cyber risk analytics, this requires that machines evolve into CPS [43].

3.1.4 Life cycle and anti-counterfeit for artificial intelligence for cyber risk analytics—SCRM

This needs task-specific human machine interfaces [44], for self-aware machines and component prognostics and health management [45].

3.1.5 Diminishing manufacturing sources, material shortages and supply chain risk management—LCM

This is required for prioritising and optimising decisions with self-optimising production systems [46], supported with production-planning computer visualisation, such as SCADA systems integration with virtual reality [47] for developing the decision support system.

3.1.6 Software assurance and application security for artificial cognition—SAAS

This requires a big data platform [48, 49] for sensors condition-based monitoring. Such platforms can enable complex models, such as cyber city designs [50] using structured communications for mobile CPS [51], cross-domain end-to-end communication among objects and cloud computing techniques.

3.1.7 Forensics, prognostics and recovery plans for artificial cognition—FPR

This needs to be informed by key performance indicators [52].

3.1.8 Track and trace in cyber risk analytics—TaT

Feedback and control mechanisms are required for enabling supervisory control of actions, to avoid or grant required access or to design a resilient control system [53].

3.1.9 Anti-malicious and anti-tamper—AMAT

This would be facilitated with loosely time-triggered architectures [54] and structure dynamics control.

3.2 Taxonomy of requirements for artificial intelligence for CPS in manufacturing and 'servitization'

The requirements for AI for CPS in manufacturing and 'servitization' are presented in a taxonomy with abbreviations (Table 1) that support a robust integration of artificial intelligence for the cyber risk analytics. The taxonomy presents the requirements for AI identified in the literature on predictive cyber risk analytics, where AI components and connectors service the entire system at runtime.

The taxonomy of requirements in Table 2 for artificial intelligence for CPS in manufacturing and 'servitization', enables a holistic understanding of the requirements for integrating cognitive CPS in the cyber risk analytics with dynamic real-time data from manufacturing and 'servitization'. The grouping of requirements is used in the following section to analyse the required applications and technologies and to build a cascading architecture for integrating artificial intelligence for CPS. This topic was identified as imperative in the engineering literature [53], for assessing the impact of IoT cyber risks.

Table 2 Taxonomy of requirements for artificial intelligence for CPS in manufacturing and 'servitization'

Self-maintaining connection	
Software assurance and application security	
Big data platform	BDP
Mobile CPS	mCPS
Required:	
Condition-based monitoring	CBM
Self-aware conversion	
Life cycle and anti-counterfeit	
Task specific human machine interfaces	HMI
Self-aware machines and components	MaC
Anti-malicious and anti-tamper	
Loosely time-triggered architectures	LTTA
Structure dynamics control	SDC
Required:	
Prognostics and health management	PHM
Cyber self-compare	
Electronic and physical security	
Real-time data acquisition and storage solutions	RTD
Fleet of machines	FoM
Adaptive analysis	AA
Peer-to-peer monitoring	PtPM
Required:	
Cyber-physical systems	CPS
Self-predicting cognition	
Diminishing manufacturing sources, material shortages and supply chain risk management	
Prioritising and optimising decisions	POD
Self-optimising production systems	SOPS
Information assurance and data security	
Autonomous cognitive decisions	ACD
Machine-learning algorithms	MLA
High-performance computing for data analysis	HPC
Information sharing and reporting	ISR
Required:	
Decision support system	DSS
Self-organising and self-configuring	
Track and trace	
Supervisory control of actions to avoid or grant access	CoA
Forensics, prognostics and recovery plans	
Key performance indicators	KPI
Asset management and access control	
Cyber-physical production systems	CPPS
Required:	
Resilient control system	RCS

4 Design and prototype of AI-enabled dynamic cyber risk analytics at the edge

From applying the grounded theory to design a taxonomy of future requirements, a new design emerges for the future role of AI in CPS, which includes (1) self-maintaining machine connections for acquiring data and selecting sensors; (2) self-awareness algorithms for the conversion of data into information; (3) connecting machines to create self-comparing cyber networks that can predict future machine behaviour; (4) the capacity to generate cognitive knowledge of the system to self-predict and self-optimise before transferring knowledge to the user; and (5) a configuration feedback and supervisory control route from cyberspace to physical space, that allows machines to self-configure, self-organise and to be self-adaptive.

The emerging applications and technologies in Table 3 are presented in the form of a cascading framework in Fig. 2 to hierarchically organise their relationships in artificial intelligence for CPS. Grounded theory is applied to identify the hierarchy of order as identified in the taxonomy. Figure 2 presents the way machines can connect to the cognitive CPS and exchange information through cyber network [55] and provide optimised production and inventory management [56] and lean production [57].

The categorisation in Table 3 is derived from applying grounded theory to categorise concepts from the existing literature. The principles of grounded theory demand that all prominent themes need to be categorised, hence the emergence of a 'cyber' category. However, from our perspective on cyber security engineering, the cascading framework contains one error, which is also present in the literature reviewed. The error is that referring to the middle layer as 'cyber' demonstrates a different understanding to that we find in cyber security engineering. Current developments in industrial systems refer to cyber elements that are now extending from sensor/actuator through to supervisory control and advanced analytic solutions. The grounded theory principles state that we need to report what we observe, not what we think it is correct or incorrect and since cyber is a buzz word, it can refer to many things. The literature should probably be reworded, but the taxonomy is based on grounded theory and the fundamental principles of grounded theory are applied to categorise themes from the existing literature. This error in effect exposes a significant weakness in the current juxtaposition in the literature of many related systems and technologies.

Nevertheless, regardless of our disagreement with the naming one category in Fig. 2, the described cascading architecture represents a cognitive architecture. The cognitive architecture allows for learning algorithms and technologies to be changed quickly and reused on different platforms [58] which is necessary in usual CPS situations, such as when creating multi-vendor and modular

Table 3 The applications and technologies related to artificial intelligence for CPS

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

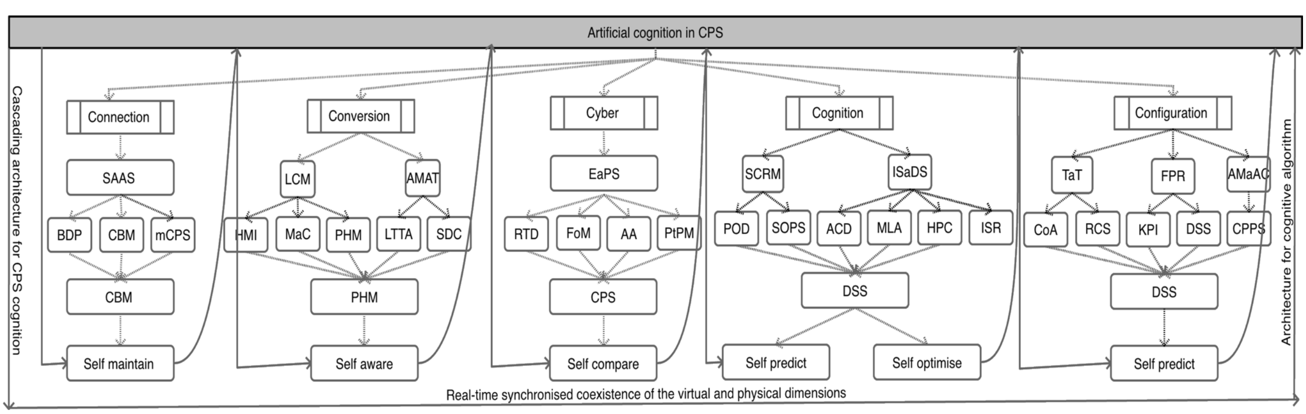

Fig. 2 Cascading framework for artificial intelligence for CPS

production systems. Such reuse can be achieved through VEO and VEP in CPS, which enable the real-time synchronised coexistence of the virtual and physical dimensions (see [59]). The emergence of a flaw in the juxtaposition in the literature in the process of categorising elements of the CPS cognition confirms that CPS design requires multi-discipline testing and verification, including system design and system engineering (see [60]), and requires an understanding of system sociology [61]. The proposed cascading architecture operates in a similar method with social networks, in the sense that individuals can influence the production line.

The future developments for artificial intelligence for CPS as presented in Fig. 2, include instruments and processes to enable energy-aware buildings and cities (EABaC); physical critical infrastructure with preventive maintenance (CIPM); and self-correcting cyber-physical systems (SCCPS) themselves. In addition, the electric power grid represents one of the largest complex interconnected networks [62]. Under stressed conditions, a single failure can trigger complex cascading effect, creating wide-spread failure and blackouts. Flexible AC transmission systems would enable protection against such cascading failures and distributed energy resource technologies [63] such as wind power, create additional stress and vulnerabilities.

4.1 Discussion

The cascading framework in Fig. 2 presents a new way to design dynamic and automated predictive systems supported with real-time intelligence. This framework supports an assessment of the potential for adapting AI cognitive engines in data collection and analytics with dynamic real-time feedback. These engines might provide predictive intelligence on threat event frequency and the potential magnitude of resulting losses. Undoubtedly, to provide this functionality, deep learning algorithms need to be adopted into cognitive engines to form dynamic confidence intervals and time bound ranges with real-time data. Once we have these abilities the cascading framework in Fig. 2 becomes a modern tool for risk analytics.

To test whether our proposed framework is more effective or academically valuable than the traditional classification method, we used the case study method in combination with the grounded theory. This study was funded by Cisco Systems, and we conducted three scoping and verification workshops together, at which we presented our proposed framework, in comparison with the existing framework on CPSs [37]. At these workshops, our proposed framework was judged to be more effective or academically valuable than the traditional classification method, in that it includes concepts that have emerged since the existing framework on CPSs [37] was established in 2015. Our proposed framework is, in other words, an updated version that includes new technological concepts that have emerged since the establishment of the existing framework in 2015 [37].

5 Conclusion

The integration of AI into cyber physical systems has resulted in the rapid emergence of research, and a juxtaposition in the literature reshaping not only cyber risk analytics, but also data analytics. This paper reports a new framework explaining how AI can be integrated with cyber risk analytics. This confirms that CPS design requires an understanding of system design, system engineering and system sociology.

The main findings from this paper include:

1. AI integration in communications networks and connected technology must evolve in an ethical manner that humans can understand, while maintaining maximum trust and privacy of the users;
2. The co-ordination of AI in CPS's must be reliable to prevent abuse from insider threats, organised crime, terror organisations or state-sponsored aggressors;
3. Data risk is encouraging the private sector to take steps to improve the management of confidential and proprietary information intellectual property and to protect personally identifiable information;
4. Analysis of a dynamic and self-adopting AI design for a cognition engine mechanism for the control, analysis, distribution and management of probabilistic data.

In addition to these findings, this paper applied the grounded theory to group the requirements for AI in CPS risk analytics for 'servitization' in manufacturing. The grounded theory analysis was then built into a conceptual diagram, representing a cascading hierarchy of processes.

Secondly, this paper analysed the requirements for AI in CPS 'servitization' in manufacturing and presented these in a taxonomy that supports a robust integration of cyber risk analytics. The taxonomy details the requirements, as identified in the literature, for predictive cyber risk analytics, in which AI components and connectors service the entire system during its operation. The taxonomy enables a holistic understanding of the requirements for integrating cognitive CPS in the cyber risk analytics with dynamic real-time data from manufacturing and 'servitization'.

Acknowledgements Eternal gratitude to the Fulbright Visiting Scholar Project.

Author contributions Dr. Petar Radanliev: main author; Prof. Dave De Roure, Prof. Max Van Kleek: supervision; Dr. Rafael Mantilla Montalvo, Omar Santos, La'Treall Maddox, Robert Walton, Prof. Pete Burnap, Eirini Anthi: supervision, review and corrections.

Funding This work was funded by the UK EPSRC [Grant No. EP/S035362/1] and by the Cisco Research Centre [Grant No. 1525381].

Availability of data and materials All data and materials included in the article.

Compliance with ethical standard

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict or competing interest.

References

1. Wahlster W, Helbig J, Hellinger A, Stumpf MAV, Blasco J, Galloway H, Gestaltung H (2013) Recommendations for implementing the strategic initiative Industrie 4.0. Federal Ministry of Education and Research
2. Ashton K (2011) In the real world, things matter more than ideas. RFID J 22(7):97–114
3. Gershenfeld NA (1999) When things start to think. Henry Holt, New York, NY
4. Madakam S, Ramaswamy R, Tripathi S (2015) Internet of Things (IoT): a literature review. J Comput Commun 3(3):164–173
5. Dworschak B, Zaiser H (2014) Competences for cyber-physical systems in manufacturing—first findings and scenarios. Procedia CIRP 25:345–350
6. Ringert JO, Rumpe B, Wortmann A (2015) Architecture and behavior modeling of cyber-physical systems with MontiArcAutomaton
7. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of Things (IoT): a vision, architectural elements, and future directions. Futur Gener Comput Syst 29(7):1645–1660
8. Nurse JRC, Radanliev P, Creese S, De Roure D (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: Institution of engineering and technology, living in the internet of things: cybersecurity of the IoT—2018, pp 1–9
9. Nicolescu R, Huth M, Radanliev P, De Roure D (2018) Mapping the values of IoT. J Inf Technol 33(4):345–360
10. Radanliev P, De Roure D, Nurse JRC, Mantilla Montalvo R, Cannady S, Santos O, Maddox L et al (2020) Future developments in standardisation of cyber risk in the Internet of Things (IoT). SN Appl Sci 2(2):1–16
11. Radanliev P, De Roure D, Van Kleek M, Santos O, Ani U (2020) Artificial intelligence in cyber physical systems. AI Soc 1:3
12. Mitic P (2019) Adaptive risk consensus models: simulations and applications. SN Appl Sci 1(12):1743
13. Gladson SC, Narayana AH, Bhaskar M (2019) An ultra-low-power low-noise amplifier using cross-coupled positive feedback for 5G IoT applications. SN Appl Sci 1(11):1418
14. Ibrahim H, Mostafa N, Halawa H, Elsalamouny M, Daoud R, Amer H, Adel Y et al (2019) A layered IoT architecture for greenhouse monitoring and remote control. SN Appl Sci 1(3):1–12
15. Khorshidi E, Ghezavati VR (2019) Application of mathematical modeling value-at-risk (VaR) to optimize decision making in distribution networks. SN Appl Sci 1(12):1671
16. Hariri RH, Fredericks EM, Bowers KM (2019) Uncertainty in big data analytics: survey, opportunities, and challenges. J Big Data 6(1):44
17. Kumar S, Tiwari P, Zymbler M (2019) Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6(1):111
18. Craggs B, Rashid A (2017) Smart cyber-physical systems: beyond usable security to security ergonomics by design. In: 2017 IEEE/ACM 3rd international workshop on software engineering for smart cyber-physical systems (SEsCPS), pp 22–25
19. Subroto A, Apriyana A (2019) Cyber risk prediction through social media big data analytics and statistical machine learning. J Big Data 6(1):50
20. Pääkkönen P, Pakkala D (2020) Extending reference architecture of big data systems towards machine learning in edge computing environments. J Big Data 7(1):25
21. Zhu Q, Rieger C, Basar T (2011) A hierarchical security architecture for cyber-physical systems. In: 2011 4th international symposium on resilient control systems, pp 15–20
22. Leitão P, Colombo AW, Karnouskos S (2016) Industrial automation based on cyber-physical systems technologies: prototype implementations and challenges. Comput Ind 81:11–25
23. Longstaff TA, Haimes YY (2002) A holistic roadmap for survivable infrastructure systems. IEEE Trans Syst Man Cybern - Part A Syst Hum 32(2):260–268
24. CoNSS, Committee on National Security Systems (2010) National information assurance (IA) glossary. Fort George G., Meade, MD
25. Rajkumar R, 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, p 731
26. DiMase D, Collier ZA, Heffner K, Linkov I (2015) Systems engineering framework for cyber physical security and resilience. Environ Syst Decis 35(2):291–300
27. Marwedel P, Engel M (2016) Cyber-physical systems: opportunities, challenges and (some) solutions. Springer, Berlin, pp 1–30
28. 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, p 189
29. Sokolov B, Ivanov D (2015) Integrated scheduling of material flows and information services in industry 4.0 supply networks. IFAC-PapersOnLine 48(3):1533–1538
30. Evans PC, Annunziata M (2012) Industrial internet: pushing the boundaries of minds and machines. General Electric
31. Sangiovanni-Vincentelli A, Damm W, Passerone R (2012) Taming Dr. Frankenstein: contract-based design for cyber-physical systems * g. Eur J Control 18:217–238

32. Ruan K (2017) Introducing cybernomics: a unifying economic framework for measuring cyber risk. Comput Secur 65:77–89
33. De Roure D, Page KR, Radanliev P, Van Kleek M (2019) Complex coupling in cyber-physical systems and the threats of fake data. In: Living in the internet of things (IoT 2019), p 11 (6 pp.)
34. Anthi E, Williams L, Slowinska M, Theodorakopoulos G, Burnap P (2019) A supervised intrusion detection system for smart home IoT devices. IEEE Internet Things J 6(5):9042–9053
35. Ghirardello K, Maple C, Ng D, Kearney P (2018) Cyber security of smart homes: development of a reference architecture for attack surface analysis. In: Living in the internet of things: cybersecurity of the IoT—2018, p 45 (10 pp.)
36. Asmussen CB, Møller C (2019) Smart literature review: a practical topic modelling approach to exploratory literature review. J Big Data 6(1):93
37. Lee J, Bagheri B, Kao H-A (2015) A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manuf Lett 3:18–23
38. Radanliev P, De Roure D, Nicolescu R, Huth M, Montalvo RM, Cannady S, Burnap P (2018) Future developments in cyber risk assessment for the internet of things. Comput Ind 102:14–22
39. Bhave A, Krogh B, Garlan D, Schmerl B (2010) Multi-domain modeling of cyber-physical systems using architectural views. Proc Anal Virtual Integr Cyber-Phys Syst Work
40. Shi J, Wan J, Yan H, Suo H (2011) A survey of cyber-physical systems. In: 2011 international conference on wireless communications and signal processing (WCSP), pp 1–6
41. Wan J, Yan H, Li D, Zhou K, Zeng L (2013) Cyber-physical systems for optimal energy management scheme of autonomous electric vehicle. Comput J 56(8):947–956
42. Pan M, Sikorski J, Kastner CA, Akroyd J, Mosbach S, Lau R, Kraft M (2015) Applying Industry 4.0 to the Jurong Island Eco-industrial Park. Energy Procedia 75:1536–1541
43. Weyer S, Schmitt M, Ohmer M, Gorecky D (2015) Towards industry 4.0—standardization as the crucial challenge for highly modular, multi-vendor production systems. IFAC-PapersOnLine 48(3):579–584
44. Madaan A, Nurse J, de Roure D, O'Hara K, Hall W, Creese S (2018) A storm in an IoT cup: the emergence of cyber-physical social machines. SSRN Electron J
45. Van Kleek M, Smith DA, Hall W, Shadbolt N (2013) The crowd keeps me in shape': social psychology and the present and future of health social machines. In: Proceedings of the 22nd international conference on world wide Web—WWW'13 companion, pp 927–932
46. Brettel M, Fischer FG, Bendig D, Weber AR, Wolff B (2016) Enablers for self-optimizing production systems in the context. IEEE Comput Graph 41:93–98
47. Posada J, Toro C, Barandiaran I, Oyarzun D, Stricker D, de Amicis R, Pinto EB et al (2015) Visual computing as a key enabling technology for industrie 4.0 and industrial internet. IEEE Comput Graph Appl 35(2):26–40
48. Lee J, Kao H-A, Yang S (2014) Service innovation and smart analytics for industry 4.0 and big data environment. Procedia CIRP 16:3–8
49. Hussain F (2017) Internet of things building blocks and business models. Springer, Berlin
50. Petrolo R, Loscri V, Mitton N (2016) Cyber-physical objects as key elements for a smart cyber-city. Springer, Berlin, pp 31–49
51. Almeida L, Santos F, Oliveira L (2016) Structuring communications for mobile cyber-physical systems. Springer, Berlin, pp 51–76
52. Bauer W, Hämmerle M, Schlund S, Vocke C (2015) Transforming to a hyper-connected society and economy—towards an 'industry 4.0'. Procedia Manuf 3:417–424
53. Radanliev P, De Roure D, Nurse JRC, Nicolescu R, Huth M, Cannady S, Mantilla Montalvo R (2018) Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0. In: Institution of engineering and technology, living in the internet of things: cybersecurity of the IoT, p 41 (6 pp.)
54. Benveniste A (2010) Loosely time-triggered architectures for cyber-physical systems. In: Design, automation & test in Europe conference & exhibition, Dresden, pp 3–8
55. Toro C, Barandiaran I, Posada J (2015) A perspective on knowledge based and intelligent systems implementation in industrie 4.0. Procedia Comput Sci 60:362–370
56. 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, pp 135–140
57. Kolberg D, Zühlke D (2015) Lean automation enabled by industry 4.0 technologies. IFAC-PapersOnLine 48(3):1870–1875
58. Niggemann O, Biswas G, Kinnebrew JS, Khorasgani H, Volgmann S, Bunte A (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), pp 185–192
59. Shafiq SI, Sanin C, Szczerbicki E, Toro C (2015) Virtual engineering object / virtual engineering process: a specialized form of cyber physical system for industrie 4.0. Procedia Comput Sci 60:1146–1155
60. Balaji B, Al Faruque MA, Dutt N, Gupta R, Agarwal Y (2015) Models, abstractions, and architectures. In: Proceedings of the 52nd annual design automation conference on—DAC '15, pp 1–6
61. Dombrowski U, Wagner T (2014) Mental strain as field of action in the 4th industrial revolution. Procedia CIRP 17:100–105
62. Hahn A, Ashok A, Sridhar S, Govindarasu M (2013) Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans Smart Grid 4(2):847–855
63. Ahmed SH, Kim G, Kim D (2013) Cyber physical system: architecture, applications and research challenges. In: 2013 IFIP wireless days (WD), pp 1–5