# From mechatronics to the Cloud

David Bradley
David Russell
Peter Hehenberger
Jorge Azorin-Lopez
Steve Watt
Christopher Milne

This is the Author's Accepted Manuscript of the book chapter:

Bradley, D., Russell, D., Hehenberger, P., Azorin-Lopez, J., Watt, S. & Milne, C. (2020) 'From mechatronics to the Cloud'. In X.T. Yan, D. Bradley, D. Russell & P. Moore (eds.), *Reinventing mechatronics: developing future directions for mechatronics*. Springer, Cham, pp. 17-33.

The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-030-29131-0_3

# From Mechatronics to The Cloud

**David Bradley[†], David Russell[‡], Peter Hehenberger[*], Jorge Azorin-Lopez[¶], Steve Watt[§] & Christopher Milne[§]**

[†] Abertay University, UK
[‡] Penn State Great Valley, USA
[*] University of Applied Sciences Upper Austria, Austria
[¶] University of Alicante, Spain
[§] University of St Andrews, UK

## Abstract

At its conception mechatronics was viewed purely in terms of the ability to integrate the technologies of mechanical and electrical engineering with Computer Science to transfer functionality, and hence complexity, from the mechanical domain to the software domain. However, as technologies, and in particular computing technologies, have evolved so the nature of mechatronics has changed from being purely associated with essentially stand-alone systems such as robots to providing the smart objects and systems which are the building blocks for Cyber-Physical Systems, and hence for Internet of Things and Cloud-based systems. With the possible advent of a 4th Industrial revolution structured around these systems level concepts, mechatronics must again adapt its world view, if not its underlying technologies, to meet this new challenge.

## How did we get to here?

The concept of a central repository of computational power and associated storage and systems of this nature were historically used by companies and universities to support remote users [1]. As the internet became increasingly available, so distributed computer power in the form of client-server architectures emerged when information could be streamed to and from a user and the interaction between the computer centre and a remote user eventually evolved into internet transactions packages [2,3].

The web-based information industry is now invisibly connected to remote servers, data banks, and platforms with The Cloud providing application and distribution centres [4]. Information-heavy industries such as banks, investment houses, and government agencies were frontrunners in this mode of operation followed by online retailers, virtual video game systems, voice-over internet protocols (e.g. Skype®) and search engines such as Siri® and Google®. This was followed by the introduction of remotely accessible smart devices or objects capable of being used for a range and variety of purposes such as environmental control, the opening and closing of garage doors, or activating and querying alarm systems [5].

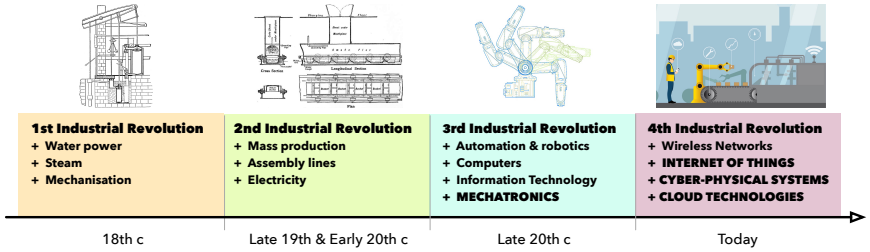


**Fig. 1.** Timeline of Industrial Revolutions.

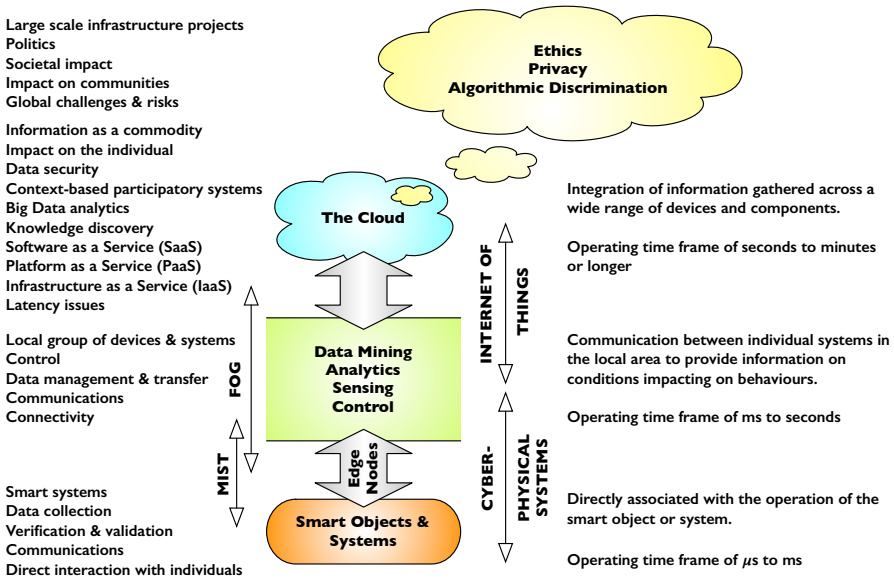


**Fig. 2.** From mechatronic smart objects and systems to The Cloud.

## Mechatronics, Cyber-Physical Systems, the Internet of Things & The Cloud

As suggested by Fig. 1, mechatronics was a major driver of and for the 3rd Industrial Revolution, itself structured around computing, information technology and robotics, that began around 1970. However, the advent of a 4th Industrial Revolution configured around Cyber-Physical Systems (CPS) [6], the Internet of Things (IoT) [7], Cloud technologies [8] and elements of Big Data [9] means that mechatronic devices and systems must now be configured to provide the intelligent or smart components and objects with which such a system is built.

To put this emerging and evolving role for mechatronics into context, consider the structure of Fig. 2 and the system exemplars of Table 1 which bring together these various elements and identifies the relationships between the layers in the resulting hierarchy. What is then immediately clear is that there is a requirement for on-demand access to a range of resources including infrastructure, software and platforms with the resulting system a dynamic entity with smart objects and users entering and leaving dependent on both context and need. This then means that both data and information become commodities to be traded by the system on request. Thus for instance, knowledge that a traffic incident is resulting in delays is only of value to a user if they were intending to travel on affected roads.

**Table 1.** System exemplars

| | Exemplar 1 - Manufacturing System | Exemplar 2 - Vehicle Systems |
|---|---|---|
| Mechatronic Smart Objects & Systems | Individual machine tools and robots serviced by autonomous guided vehicles.<br>Each tool or robot carries out a task or tasks in accordance with the production schedule. | Individual vehicle sub-systems & components such as engine management, traction control, environmental controls, entertainment and communications systems. |
| | **Operating time frame of µs to ms and possibly seconds** | |
| Cyber-Physical System | Task based groupings of machine tools & robots<br>Islands of Automation<br>Local materials transfer and transport<br>Task scheduling<br>Condition monitoring & reporting | The complete vehicle integrating all on board systems at various levels such as:<br>Driver support – Cruise control, autonomous headlights, blind-spot alert, etc.<br>Driver assistance – Self-parking, emergency braking, etc.<br>Autonomous operation<br>As determined by installed software |
| | **Operating time frame of ms to seconds and possibly longer** | |
| Internet of Things | Factory wide scheduling<br>Materials transfer & transport<br>Inventory management | Communication with other vehicles in vicinity<br>Traffic alerts<br>Routing information |

| | Materials incoming & despatch | Parking requests & allocation |
|---|---|---|
| | **Operating time frame of seconds to minutes and possibly longer** | |
| Cloud | Data storage & analysis | Data storage & analysis |
| | Big Data analytics | Big Data analytics |
| | Performance data collection | Performance data collection |
| | Inventory control | Fault detection across fleet |
| | Order handling | Digital twin |
| | Production planning | Traffic management systems |
| | **Operating time frame of seconds to minutes, hours or even days depending on context** | |

Other system elements included in Fig. 2 are:

*Edge Nodes* – Support the operation of smart devices or components by avoiding the need to send information to the cloud for processing, thus avoiding network latency effects.

*Mist Layer* – Provides an interface between the local processing associated with the edge nodes and the Fog.

*Fog Computing* – This is defined by the National Institute of Standards and Technology (NIST) in the US as [10]:

> "… a horizontal, physical or virtual resource paradigm that resides between smart end-devices and traditional cloud or data centres. This paradigm supports vertically-isolated, latency-sensitive applications by providing ubiquitous, scalable, layered, federated, and distributed computing, storage, and network connectivity."

Features of Fog Computing include [10-14]:

*Distribution* – Supports highly distributed services.

*Cloud to Things* - Fog nodes are positioned close to functional smart objects so that analysis and response times are reduced.

*Horizontal Architecture* – Supports multiple application domains.

*Interoperability* **-** Seamless service support requires the co-operation of different providers implying interoperability and the federation of services.

*Mobility* - Directly associated with mobile devices.

*Real-Time Functionality* – Analysis in real-time of streamed data.

*Sensor Networks* – Includes real-time validation and verification.

## Design Issues

Conventionally, the design of complex engineering systems followed a structured path in which the design and development stages, including those for sub-assemblies or sub-components, were linked to the implementation stages by validation and verification procedures intended to confirm performance to specification. The net result is that all system elements, hardware, software and firmware, are developed under the overall control and responsibility of the design team. This design pathway is increasingly being challenged by developments in mechatronics and Cyber-Physical Systems (CPSs) and their links to the Internet of Things (IoT) and The Cloud in which the transition from the (mechatronic) component to a CPS and the IoT results in increasing levels of abstraction, limiting the ability of the design team to maintain control over, or even input to, the entirety of the system. This means that those system elements drawn from the cloud will in general be unknown to the designers of smart (i.e. mechatronic) sub-assemblies and components while still being required to establish and define system functionality [5], a situation illustrated here by Fig. 3 when insertion of a new component can result in an, albeit unintended, system failure.

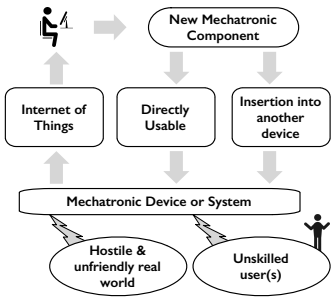


**Fig. 3.** From design to real-world.

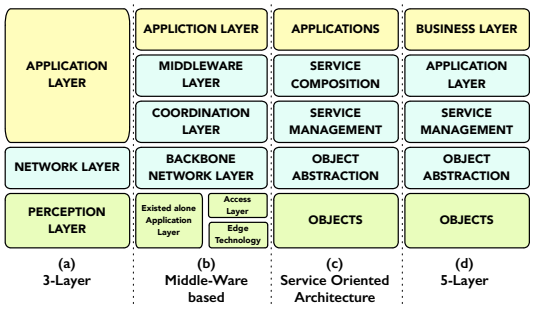


**Fig. 4.** Potential IoT architectures {after [15]}

The range and scope of the challenges facing the designer can be expressed by reference to the World Economic Forum Report '*Deep Shift - Technology Tipping Points and Societal Impact*' [16] which identified the major areas of impact upon society being those set out in Table 2:

**Table 2.** Potential for societal impact

| | |
|---|---|
| *People & the Internet* | How people connect with others, information and the world around them is being transformed. Wearable and implantable technologies will enhance an individual's "*digital presence*", allowing them to interact with objects and each another in new ways. |
| *Universal Computing,* | The continued decline in the size and cost of computing and connectivity technologies is driving an exponential growth in the potential to access and |

| | |
|---|---|
| *Communications & Storage* | leverage the internet. This will lead to the availability of ubiquitous computing power where everyone has access to a supercomputer in their pocket, with nearly unlimited storage capacity. |
| *Internet of Things* | Smaller, cheaper and smarter sensors are being introduced in homes, clothes and accessories, cities, transport and energy networks, as well as in manufacturing. |
| *Artificial. Intelligence & Big Data* | Exponential digitisation creates exponentially more data about everything and everyone. The sophistication of the problems that can be addressed, and the ability for software to learn and evolve, is advancing in parallel. |
| *Sharing Economy & Distributed Trust* | The internet is driving a shift towards networks and platform-based social and economic models, creating not just new efficiencies but also whole new business models and opportunities for social self-organisation. |
| *Digitisation of Matter* | 3D printing as a process that transforms industrial manufacturing and allows for home based production. It also creates a new set of opportunities for human health. |

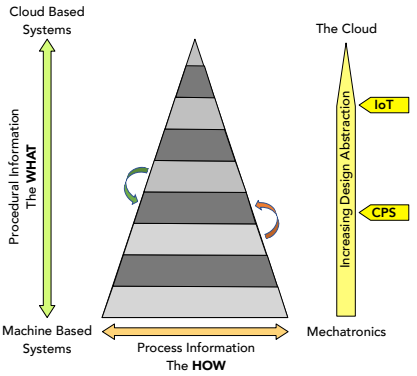


**Fig. 5.** Procedural and Process information based system representation.

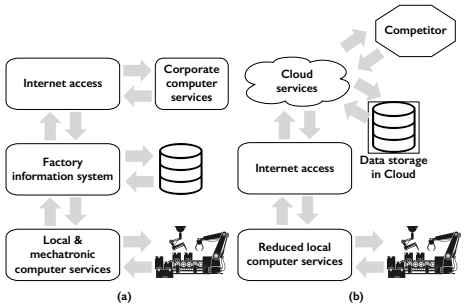


**Fig. 6.** Manufacturing systems (a) Self contained and (b) Cloud based

## What Does What?

The increasingly distributed nature of systems involving the IoT and the Cloud has resulted in consideration of the potential architectures for such systems [17,18,19] as suggested by Fig. 4. In the context of mechatronics, the associated structural relationships can then be illustrated by Fig. 5 when mechatronics sits at the operational level of machine based systems. This suggests that the mechatronics designer must be primarily concerned with achieving the required functionality and performance at the relevant process layer whilst providing the necessary information and data to feed upwards (in terms of the model) to the CPS, IoT and Cloud levels. The translation and interpretation of data and information as it moves be-

tween the process layers is then associated with increasing levels of design abstraction as the nature, structure and context of the finally system will generally be unknown at the mechatronics layer(s).

In the context of Figs 4 & 5, this means that system intelligence is distributed throughout the system from the mechatronics layer(s) to the cloud, with each layer functioning to provide its own specific behavioural contributions within an overall system context. As mechatronic systems are the primary providers of data to the cloud, their design must take account of what is necessary to transmit the data in the form of the associated processes and protocols as well as the levels of translation and interpretation involved.

## *Manufacturing Systems*

Why is it that The Cloud and the associated IoT paradigm so limited in effectiveness in industrial mechatronic systems even in respect of Industry 4.0? Wu et al [20] proclaim that cloud based manufacturing is indeed a new exciting paradigm, while others, such as Wang et al [21], suggest that:

> "Computational cost and network communication (limitations) … present a bottleneck for effective utilization of this new infrastructure."

New technologies generally emerge from laboratories where they function flawlessly under the guidance of their designers, and even beta test sites are generally friendly towards the technology. Referring back to Fig. 3, is not just the learning curve of the untrained user, or the integration of new technology into some existing application, that determines outcomes in service but the influence of what, in contrast to the laboratory, is often a hostile, demanding and unfriendly physical environment.

Since the industrial revolution, automation has increasingly featured in the operation and development plans of manufacturing and smart devices are now found in factories which when operating promote higher quality products for ever more selective customers. Components such as automated materials handling, packing, autonomous vehicles and flexible groupings of robots and machine tools all contribute to outcomes, yet are usually reliant on local computational support as suggested by Fig. 6(a) with information access to and by the outside world restricted to order processing, job scheduling and product delivery. Here, local computing supplies schedules, order data, and inventory management with information fed to the shop floor to set up machines and transfer production data.

In contrast, Fig. 6(b) illustrates a cloud-based system, and shows the potential risk presented by a competitor being able to access company data. Access to large data sets may have significant commercial value but data centres are very expensive to fund, design and operate and the data they contain is vulnerable to access by others than for whom it was intended. Further, the inherent latency associated with

the transmission of data to and from The Cloud means that it cannot, as demonstrated by Figs 7 & 8, be used to directly control shop floor operations and Cloud-based systems thus tend to be more closely integrated with strategy than operations.

Indeed, the small to medium enterprises (SME) which constitute a very large proportion of manufacturing, may only have one or a two facilities and consequently are not financially or strategically interested in cloud systems and as they are often suppliers of key components to larger clients there is the danger of their secrets being revealed to competitors. The number of such firms is large; in 2014 in the USA, over 97% of manufacturing was associated with firms employing under 500 employees [22], and many have fewer than 50.

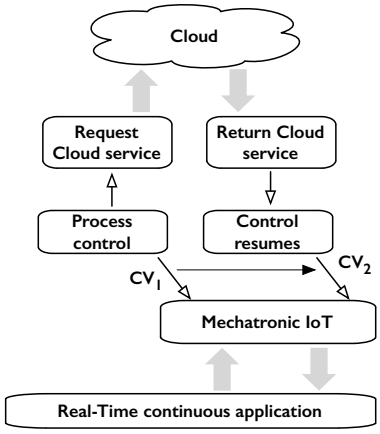


**Fig. 7.** Cloud-serviced control.

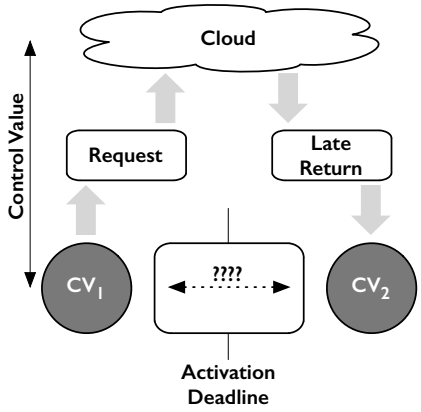


**Fig. 8.** Timing uncertainty

## Issues & Concerns

### *Privacy*

Historically, less consideration has been given to the '*softer*' or people oriented aspects of individual privacy and there is now a growing imperative to ensure data security and user privacy [23-27] within and as part of the design process [28,29,30] while ability to apply big data analysis tools to the generated data creates further questions [31].

In respect of the privacy of the individual, as opposed to the security of the system, the '*always on*' society continues to demand greater connectivity at higher speeds. In such an environment, the requirement is that connection to the local network, and hence to the Internet of Things, is essentially seamless. The resulting

operational shift from device management to data management suggests that conventional approaches to network security and individual privacy are no longer acceptable or viable, and that securing networks now requires more focus on securing what is important rather than trying to implement a lockdown approach intended to secure everything. This is particularly the case for Cloud-based systems structured around mechatronics, CPS & the IoT which are autonomously communicating and receiving information on behalf of their user.

Many of the devices and systems associated with the IoT have the capability to rapidly accumulate large volumes of personal data, much of which is likely to be held in locations and ways unknown to the user. This data is then subject to the possibility of analysis using the techniques and methods of Big Data [32,33,34], with a significant risk of impacting on the privacy of individuals [35]. Of concern is the potential to use inference to suggest personal details and behaviour. A simple instance of this is the recommender systems used as a marketing tool by companies such as *Amazon* [36] which use information derived from past customer purchases and search profiles to generate focused advertising. Other examples include:

- The potential to use information derived from, say, traffic routing apps or vehicle systems linked to domestic environmental controls to identify if a house is currently occupied.
- The potential use of information derived from eHealth systems to determine an individual's ability to access or purchase elements of healthcare provision.

The ability to analyse large volumes of data to extract potentially beneficial knowledge, particularly within the context of IoT based applications such as eHealth, for instance to provide an early warning of an impending outbreak of an infectious disease based on consolidated eHealth data, presents a major challenge to the concepts of individual privacy, and hence to system designers. And of course, there is also the potential for other, more nefarious, activities and actions based on accumulated individual data. These concerns have led to the concept of '*Digital or Algorithmic Discrimination*' [5,37-40] where the use of an individual's personal data within a Big Data algorithm leads to their being in some significant degree being discriminated against, for instance by being denied access to specific services, or being unreasonably targeted in some way. In illustration O'Neill [5] provides (from among others) the following examples:

- For profit colleges in the US used algorithms to generate advertising targeted at poorer and disadvantaged households to enable the college to access government funding at 90%.
- The use of geographically oriented law enforcement management programs such as *PredPol* and *CompStat* led to an emphasis on nuisance crimes in poorer neighbourhoods rather than on more serious crimes elsewhere.

In broad terms, discrimination is defined as the unfair treatment of an individual because of their membership of a particular group and in this context, algorithmic profiling for the allocation of resources can be considered as inherently discriminatory when data subjects are grouped into categories according to selected variables,

and decisions made on the basis of subjects falling within defined groups. In this context, machine learning can reinforce existing patterns of discrimination. If these are embodied in the training dataset, then they will be reproduced by the classifier with biased decisions presented as derived from an '*objective*' algorithm. It is a requirement that data controllers act to prevent such discriminatory effects when processing sensitive data which can include or encompass a wide range of personal information as for instance [40]:

- Racial or ethnic information.
- Religious or other beliefs.
- Membership of organisations such as trade-unions.
- Genetic or biometric data.

Whatever the ultimate outcome of the continuing legislative debate over privacy, it is clear that there is an increasing burden on system designers to place privacy at the core of their work, and that this must be reflected in changes to the design process and the associated methods and tools used to support this [41]. This brings with it concerns in relation to the ability of current best practice to accommodate the intent of legislation, and hence to meet guidelines.

## *The Consumer*

The impact of mechatronics is increasingly being felt at the consumer level and mechatronic devices are common in cars (driverless and otherwise), haptic video game consoles, self-focusing automatic cameras, home security systems, smart cities, smart houses, medical robots and a multitude of other applications. Mobile technology enables the locking of house doors remotely and checking the interior remotely while on holiday, or checking how many footsteps a person makes that day as part of a wellness program, and broadcasting that to the web for comparison with others[1].

The ability to establish an individual's location from a satellite and a mobile phone, be it turned on or not, has introduced many benefits, but also creates a whole new set of privacy issues [42]. For instance, knowledge of an individual's location and behaviour can be used to establish when they are away from home, and hence when their home is vulnerable. The implication is therefore that consumer mechatronics must not only complement the users' world, but must also autonomously adapt to unplanned circumstances and situations while recognising and responding to physical, legal and other constraints to act responsibly within an appropriate time frame.

[1] See for instance www.strava.com (as of October 2018)

## *Ethics*

Within the system structure of Fig. 2, ethical issues exist at a number of levels.

### Smart Object, Smart Device or Cyber-Physical System

Consider the following scenario involving an autonomous vehicle[2]:

> "It's a bright, sunny day and you're sitting back in your self-driving vehicle travelling at the speed limit along a tree lined road. A school bus, driven by a human, is travelling towards you and suddenly veers into your path. There is no time to stop safely, and no time for you to take control of the car."

Does the car:

- Swerve sharply into the roadside trees, possibly killing you but possibly saving the bus and its occupants?
- Perform an evasive manoeuvre around the bus and into the oncoming lane, saving you, but sending the bus into the trees and possibly killing the driver and some of the children on board?
- Hit the bus, possibly killing you as well as the driver and children on the bus?

Whatever choice is made there is the likelihood that someone will be killed, so what should the autonomous vehicle do? Whatever decision is made, it needs to be made in a time frame of μs to ms [44,45]!

### Mist and Fog Layers

At the next level up in the hierarchy of Fig. 2 and Table 1, that of the Mist and Fog layers, with information being shared with other vehicles and systems in the immediate vicinity, other questions arise as for instance how to allocate parking spaces to vehicles that request them, first-come, first-served or on some preferential basis.

Imagine now an autonomous vehicle in an urban area whose passenger has lost consciousness[3], should the vehicle now attempt to get to the hospital as fast as possible, and if so what is the risk to other road users and pedestrians? In this case, actions in the Mist and Fog Layers can act to warn other users and to clear a passage for the vehicle. Here connectivity acts to reduce risk, but not without the need to address ethical issues associated, for instance, with the assessment of absolute and relative risk for the particular set of circumstances [46].

---

[2] Adapted from [43]

[3] Detected by the on-board sensors!

### The Cloud

Cloud based ethical concerns and issues [47.48] are primarily with the ability to access and analyse the data collected by the system, including the risk, as discussed earlier, of algorithmic discrimination.

### Trust

Studies by the World Economic Forum [49] have suggested a general lack of confidence in the way in which the internet, and by implication the Internet of Things and Cloud-based systems are both structured and operated. Here, Fig. 9 shows user responses to questions as to how their levels of trust could be increased with respect to the way in which their personal data is managed. The leading areas for change are seen to be associated with the ways in which personal data might be accessed, either by security breaches or by some form of data sharing and the ways in which such data might be used. When taken together with issues such as digital (algorithmic) discrimination, this again indicates the need for mechatronics designers, as mechatronic components and systems are in general the primary data sources, to consider privacy issues from the very beginning of the design process.

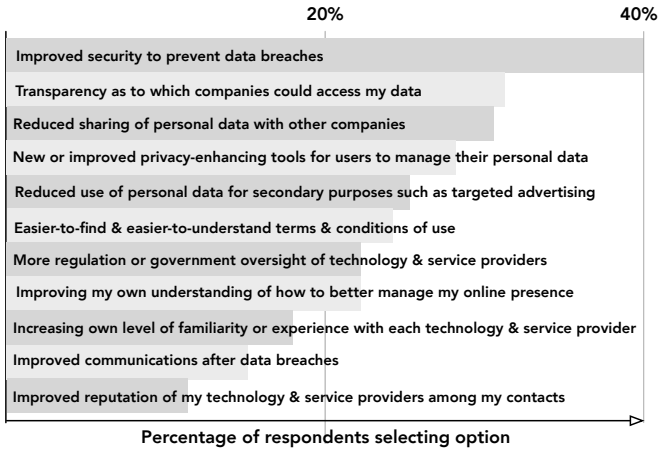


**Fig. 9.** User perception of changes required to improve trust of technologies and service providers {after [49]}

## Conclusions

In a recent article, Xu [50] suggested that:

> "Cloud computing is changing the way industries and enterprises do their businesses in that dynamically scalable and virtualized resources are provided as a service over the internet. Specifically:
> - Cloud computing is emerging as a major enabler for the manufacturing industry.
> - Cloud computing technologies can be adopted in manufacturing.
> - Cloud manufacturing is a pay-as-you-go business model.
> - Distributed resources are encapsulated into cloud services and managed centrally."

What is missing from this argument is that many manufacturing machines are intrinsically *mechatronic* and already include mechanical, electrical, computing and intelligent components. If machines need skilled attention to keep them running, regardless of where its data is sourced, there is little benefit to be gained from complicating what currently works! Thus while it is true that on the corporate level cloud-based systems have much to offer in regard to planning and strategy, at the operational level there may be little gain, especially if the skilled workforce has been reduced at both the factory floor and professional levels.

In looking at what is required, consider that Albert Einstein once commented that:

> "We cannot solve our problems with the same thinking that we used when we created them",

so how then should mechatronics be rethought, and indeed reinvented, to accommodate the demands of Cyber-Physical Systems, the Internet of Things and The Cloud.

While a sound education in mathematics and systems engineering will always be a requirement for a mechatronics design engineer, rather than just creating "*smarter mousetraps*," perhaps research and development should be equally targeted towards usability, longevity and sustainability [51,52]. Our throw-away society, in which defects and faults are excused and deferred to the next model or revision, unfortunately remains largely unaware of such concerns.

The paper has looked at some of the challenges facing a mechatronics in the era of Cyber-Physical Systems, the Internet of Things and Big Data and has attempted to isolate issues of concern and challenge facing systems designers, practitioners and legislators regarding privacy and ethical concerns in relation to the interaction between such systems as well as identifying contributing technical issues.

## References


1. Dorogovtsev SN & Mendes JF (2002) Evolution of networks, *Advances in Physics*, **51**(4), 1079-1187
2. Mattern F & Floerkemeier C (2010) From the Internet of Computers to the Internet of Things, In *From Active Data Management to Event-Based Systems and More*, Springer, 242-259
3. Dhamdhere A & Dovrolis C (2011) Twelve years in the evolution of the internet ecosystem, *IEEE/ACM Trans. on Networking*, **19**(5), 1420-1433

4. Foster I, Zhao Y, Raicu I & Lu S (2008) Cloud computing and grid computing 360-degree compared, *IEEE Grid Computing Environments Workshop (GCE'08)*, 1-10
5. Bradley DA, Russell D, Ferguson I, Isaacs J & White R (2015) The Internet of Things – The Future or the end of Mechatronics, *Mechatronics, 27*, 57-74
6. Lee EA & Seshia SA (2016) *Introduction to embedded systems: A cyber-physical systems approach*, MIT Press
7. Minerva R, Biru A & Rotondi D (2015) Towards a definition of the Internet of Things, *IEEE Internet Initiative*, 1, 1-86
8. Rittinghouse JW & Ransome JF (2016) *Cloud computing: implementation, management, and security*, CRC Press
9. Chen H, Chiang RH & Storey VC (2012) Business intelligence and analytics: from big data to big impact, *MIS Quarterly*, 1165-1188.
10. Iorga M, Feldman L, Barton R, Martin MJ, Goren N & Mahmoudi C (2017) *The NIST Definition of Fog Computing (Draft)*, NIST Special Publication 800-191
11. Datta SK, Bonnet C & Haerri J (2015) Fog Computing architecture to enable consumer centric Internet of Things services, *IEEE Intl. Symp. Consumer Electronics (ISCE),* 1-2, 2015
12. Yi S, Li C & Li Q (2015) A survey of fog computing: concepts, applications and issues, *Proc. 2015 Workshop on Mobile Big Data*, 37-42, 2015
13. Gupta H, Vahid Dastjerdi A, Ghosh SK & Buyya R (2017) iFogSim: A toolkit for modelling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments, *Software: Practice & Experience*, *47(9),* 1275-1296
14. Munir A, Kansakar P & Khan SU (2017) IFCIoT: integrated fog cloud IoT architectural paradigm for future internet of things, *IEEE Consumer Electronics Magazine,* **6**(3), 74-82
15. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M & Ayyash M (2015) Internet of things: A survey on enabling technologies, protocols, and applications, *IEEE Communications Surveys & Tutorials*, **17**(4), 2347-2376
16. World Economic Forum Report Survey Report (2015) *Deep Shift - Technology Tipping Points and Societal Impact @* www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (accessed 20 December 2017)
17. Botta A, De Donato W, Persico V & Pescapé A (2016) Integration of cloud computing and internet of things: a survey, *Future Generation Computer Systems*, 56, 684-700
18. Weyrich M & Ebert C (2016) Reference architectures for the Internet of Things, *IEEE Software*, **33**(1), 112-116
19. Yang Z, Yue Y, Yang Y, Peng Y, Wang X & Liu W (2011) Study and application on the architecture and key technologies for IoT, *IEEE Intl. Conf. Multimedia Technology,* 747-751
20. Wu D, Rosen DW, Wang L & Schaefer D (2014) Cloud-based manufacturing: old wine in new bottles? *Procedia CIRP*, 17, 94-99
21. Wang P, Gao RX & Fan Z (2015) Cloud computing for cloud manufacturing: benefits and limitations, *ASME J. Manufacturing Science & Engineering,* **137** (4), 040901

**22.** Facts & Data on Small Business and Entrepreneurship @ sbecouncil.org/about-us/facts-and-data/ (accessed 4 October 2018)

23. Schaar P (2010) Privacy by Design, *Identity in the Information Society*, **3**(2), 267-274
24. Cavoukian A, Taylor S & Abrams ME (2010) Privacy by Design: Essential for organizational accountability and strong business practices, *Identity in the Information Society*, **3**(2), 405-413
25. Radomirovic S (2010) Towards a Model for Security and Privacy in the Internet of Things, *Proc. 1st Intl. Workshop on Security of the Internet of Things*, Tokyo
26. Weber RH (2010) Internet of Things – New security and privacy challenges *Computer Law & Security Review*, 26, 23–30
27. British Standards Institute (2017) PAS 185:2017 Smart Cities – Specification for establishing and implementing a security-minded approach, BSI
28. Roman R, Jianying Zhou & Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things, *Computer Networks*, 57, 2266–2279
29. Hui Suo, Jiafu Wan, Caifeng Zou & Jianqi Liu (2012) Security in the Internet of Things: A Review, *Proc. Intl. Conf. Comp. Sci. & Electronics Engineering*, (ICCSEE), 648-651
30. Qi Jing, AV Vasilakos, Jiafu Wan, Jingwei Lu & Dechao Qiu (2014) Security of the Internet of Things: perspectives and challenges, *Wireless Networks*, 20, 2481–2501
31. O'Neill C (2017) Weapons of Math Destruction, Penguin
32. Kambatla K, Kollias G, Kumar V & Grama A (2014) Trends in big data analytics, *J. Parallel & Distributed Computing*, **74**(7), 2561-2573
33. Hsinchun Chen, Chiang RHL & Storey VC (2012) Business Intelligence & Analytics: From Big Data to Big Impact, *MIS Quarterly*, **36**(4), 1165-1188
34. Raghupathi W & Raghupathi V (2014) Big data analytics in healthcare: promise and potential, *Health Information Science and Systems (Online),* **2**(1), 3
35. Lazer D, Kennedy R, King G & Vespignani A (2014) The Parable of Google Flu: Traps in Big Data Analysis, *Science*, 343, 1203-1205
36. Panniello U, Tuzhilin A & Gorgoglione M (2012) Comparing context aware recommender systems in terms of accuracy and diversity, *User Modelling & User-Adapted Interaction*, **24**(1), 35-65
37. Kroll JA, Barocas S, Felten EW, Reidenberg JR, Robinson DG & Yu H (2016) Accountable algorithms, *U P. Law. Review*, 165, 633-705
38. Kim PT (2017) Auditing Algorithms for Discrimination. *U. Pa Law Review Online*, **166**(1), 189 - 203
39. Danks D & London AJ (2017) Algorithmic bias in autonomous systems, *Proc. 26th Intl. Joint Conf. on Artificial Intelligence*, 4691-4697
40. Goodman BW & Flaxman S (2016) EU regulations on algorithmic decision-making and a "right to explanation". *ICML Workshop Human Interpretability in Machine Learning,* New York, 26-30
41. Landau S, Control use of Data to Protect Privacy (2015) *Science - Special issue The End of Privacy*, **347**(6221), 504-506
42. Watt S, Milne C, Bradley D, Russell D, Hehenberger P & Azorin-Lopez J (2016) Privacy Matters–Issues within Mechatronics. *IFAC-PapersOnLine*, **49**(21), 423-430

43. Spangler T (2017) Self-driving cars programmed to decide who dies in a crash, *USA Today* @ eu.usatoday.com/story/money/cars/2017/11/23/self-driving-cars-programmed-decide-who-dies-crash/891493001/ (accessed 4 October 2018)
44. Goodall NJ (2016) Can you program ethics into a self-driving car?, *IEEE Spectrum*, **53**(6), 28-58
45. Sparrow R & Howard M (2017) When human beings are like drunk robots: Driverless vehicles, ethics, and the future of transport, *Transportation Research Pt C: Emerging Technologies*, 80, 206-215
46. Bonnefon JF, Shariff A & Rahwan I (2016) The social dilemma of autonomous vehicles. *Science*, **352**(6293), 1573-1576
47. Rogers C & Duranti L (2017) Ethics in the Cloud, *J. Contemporary Archival Studies*, **4**(2), 1-11
48. de Bruin B & Floridi L (2017) The ethics of cloud computing. *Science and engineering ethics*, **23**(1), 21-39
49. World Economic Forum White Paper (2017) *Shaping the Future Implications of Digital Me*dia for Society - Valuing Personal Data and Rebuilding Trust @ www3.wefrum.org/docs/WEF_End_User_Perspective_on_Digital_Media_Survey_Summary_2017.pdf (accessed 20 December 2017
50. Xu X (2012) From cloud computing to cloud manufacturing, *Robotics & Computer Integrated Manufacturing*, **28**(1), 75-86
51. Tiefenbeck V, Tasic V, Schob S & Staake T (2013) Mechatronics to drive environmental sustainability: Measuring, visualizing and transforming consumer patterns on a large scale, *IEEE Industrial Electronics Society 39th Annual Conf.* (*IECON 2013)*, 4768-4773
52. Edwards B (2014) *Rough Guide to Sustainability: A Design Primer*, RIBA Publishing