Mechatronics & the Cloud

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

This is the authors' version of a paper presented at the *16th Mechatronics Forum International Conference: Reinventing Mechatronics*, Glasgow 19/09/18 - 21/09/18 and published in final form in the conference proceedings.

Mechatronics & The Cloud

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

*Abertay University, Dundee, UK (e-mail: dabonipad@gmail.com)
**Penn State Great Valley, Malvern, PA, USA (e-mail: drussell@psu.edu)
***University of Applied Sciences Upper Austria, Wels, Austria (e-mail: peter.hehenberger@fh-wels.at)
****University of St Andrews, St Andrews, UK (email: c.milne@st-andrews.ac.uk)
*****University of Alicante, Alicante, Spain (email: jazorin@ua.es)

Abstract: Conventionally, the engineering design process has assumed that the design team is able to exercise control over all elements of the design, either directly or indirectly in the case of sub-systems through their specifications. The introduction of Cyber-Physical Systems (CPS) and the Internet of Things (IoT) means that a design team's ability to have control over all elements of a system is no longer the case, particularly as the actual system configuration may well be being dynamically reconfigured in real-time according to user (and vendor) context and need. Additionally, the integration of the Internet of Things with elements of Big Data means that information becomes a commodity to be autonomously traded by and between systems, again according to context and need, all of which has implications for the privacy of system users. The paper therefore considers the relationship between mechatronics and cloud-based technologies in relation to issues such as the distribution of functionality and user privacy.

Keywords: Big Data, Fog Computing, Mechatronics System Design, Privacy, The Cloud

1. MECHATRONICS, CYBER-PHYSICAL SYSTEMS, THE INTERNET OF THINGS & BIG DATA

Conventional approaches to engineering design and product development tend to follow paths such as those of Fig. 1, supported by a process of requirements capture and system definition. This is followed by a process of system development founded upon appropriate testing regimes developed during the system definition phase to support validation and verification, beginning at the level of the individual sub-modules or modules and continuing to the full system level. This process is aimed at ensuring that the complete system is validated by reference to known, specified, and individually validated, components.

This approach has evolved over many years through the synergetic interaction between design theory and design practice [1]. However, it must be recognised that the identification of and explanation for effective approaches to design must inevitably lag the approaches being taken by practitioners who are exploring the possibilities afforded by new technologies without necessarily having a full understanding of their capability or implications.

As suggested in Fig. 2, Mechatronics was a major driver of the 3rd Industrial Revolution that began around 1970 and was structured around computing, information technology and robotics. However, with the advent of a 4th Industrial Revolution structured around Cyber-Physical Systems (CPS) and the Internet of Things (IoT), the role of mechatronics has to a significant degree shifted to that of providing the intelligent or smart components which constitute the
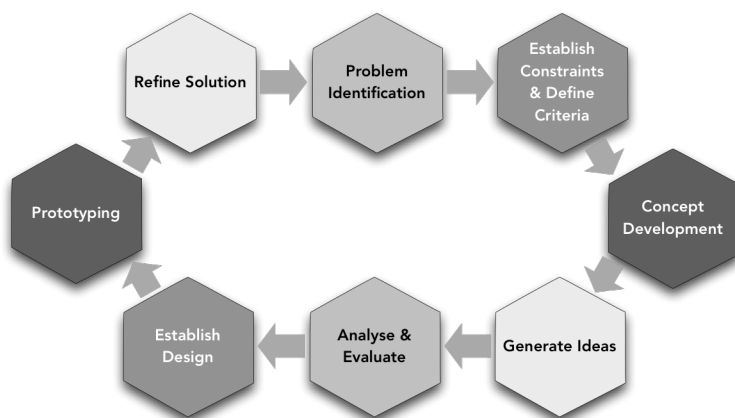
(a) Engineering design process model
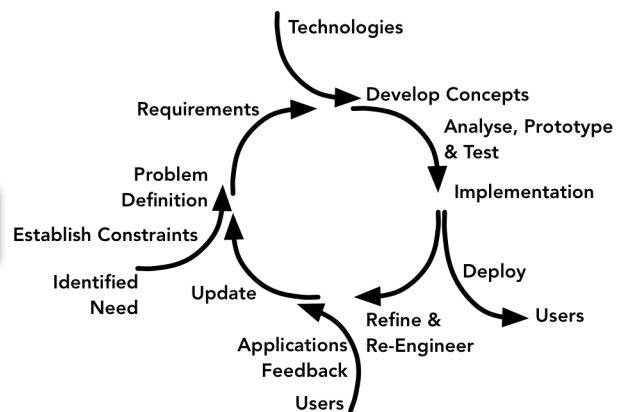
(b) Continuous product development model

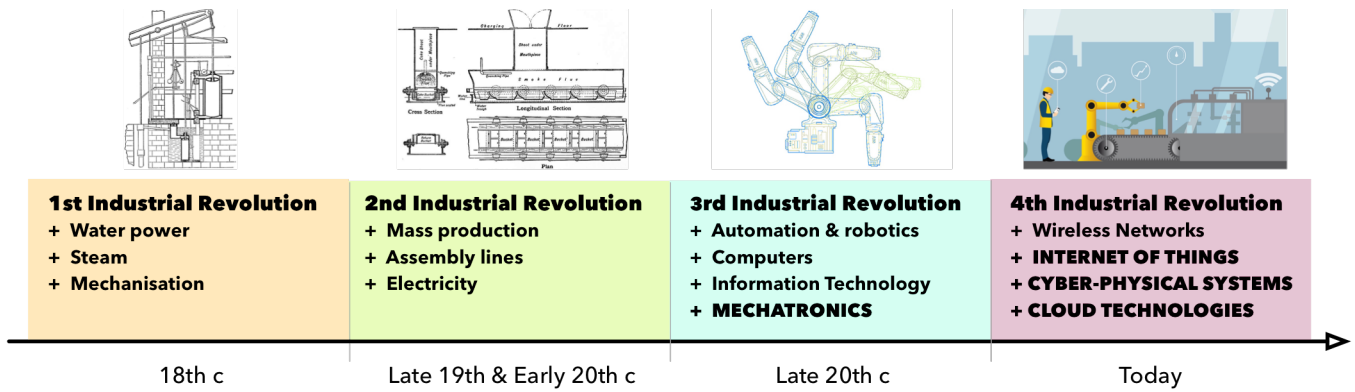Fig. 1. Product design and development models

Fig. 2. Timeline of industrial revolutions

Table 1. From Mechatronics to the Cloud

System Level	Notes
Mechatronic	The individual components making up the physical structure of the system. In the case of a vehicle, these would range from individual sensors and actuators to smart sub-systems such as engine management, traction control, braking systems and environmental control incorporating significant local levels of intelligence.
CPS	Operating under the control of the intelligent cyber component, the individual vehicle systems are brought together as a Cyber-Physical System. This enables the individual (e.g. mechatronic) components and sub-systems to operate together to facilitate and optimise system behaviour, for instance by linking the engine management, traction control and smart gear boxes to minimise fuel consumption.
IoT	Supports information exchange between individual vehicles as well as with other locations. For instance, direct communication between vehicles can be linked to traffic light control to manage traffic flow and, if required, provide clear path routing for emergency vehicles.
The Cloud	Provides access to a range of resources structured around Applications (Software as a Service (SaaS)), Platform (Platform as a Service (PaaS)) & Infrastructure (Infrastructure as a Service (IaaS)) and including Big Data analysis.

fundamental system structure. To put this shift into context, consider the relationships of Table 1 which uses vehicle systems as an exemplar of the relationships between the Mechatronics layer, the CPS layer and the IoT layer within a complex system represented diagrammatically by Fig. 3.
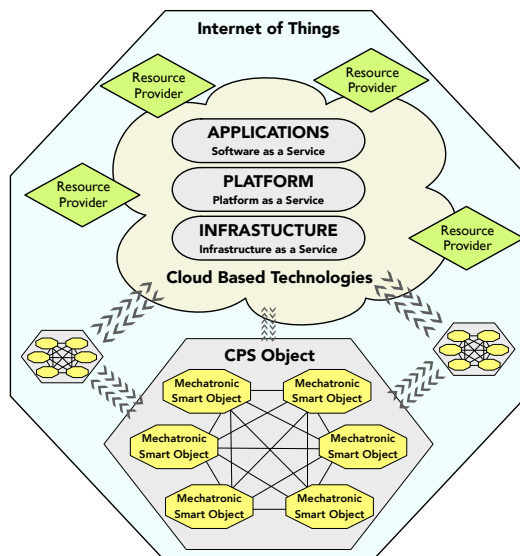

Fig.3. Mechatronics to the Cloud

In doing so it supports on demand access to a range of resources including software and platforms with the final system then being a dynamic entity with smart objects and users entering and leaving dependent on both context and need. This means that both data and information can become commodities to be traded by the system on request. For instance, the knowledge that a traffic incident is resulting in delays is only of value for some indeterminate time interval to a user of a routing system if they were intending to travel on affected roads. The system designer is thus placed in the position of having to ensure functionality without definitive knowledge of system structure, configuration or context.

2. THE DESIGNER

Conventionally, the design of complex engineering systems has followed a structured path in which the design and development stages are linked to the implementation stages by validation and verification procedures intended to establish the validity of the individual system components and their interactions. The design process also attempts to ensure that where there are sub-assemblies or sub-components that are to be integrated at the system level then their development is controlled by ensuring that they are specified appropriately. 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 cloud based systems and the Internet of Things (IoT) in which the transition from the (mechatronic) component to a CPS and the IoT results in increasing levels of

Table 2. Hard security measures

Measure	Notes
Cryptography	Public/private key encryption, digital signatures, steganography, secret sharing, key management, escrow and public & private certificates.
Firewalls	Establishes a logical barrier between a trusted and secure network and any external networks.
Passwords	Security depends on passwords being difficult to guess or discover.

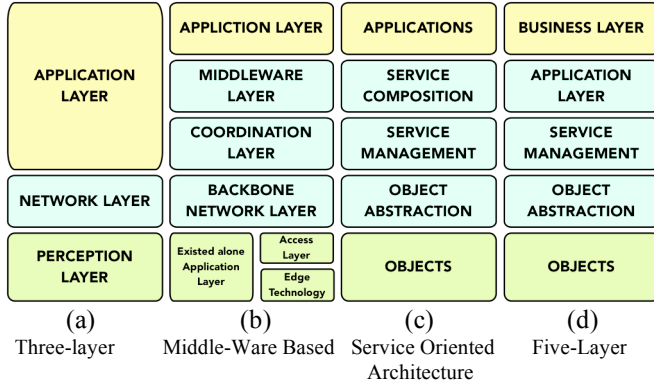| (a) Three-layer | (b) Middle-Ware Based | (c) Service Oriented Architecture | (d) Five-Layer |

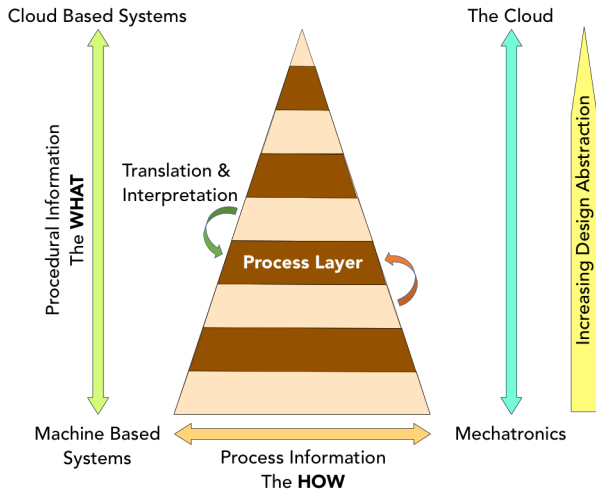Fig. 4. Potential IoT architectures {after [13]}

Fig. 5. Procedural and Process based system model

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 be unknown to the designers, who nevertheless are still required to establish and define system functionality [2]. There is also a growing imperative to ensure data security and user privacy [3,4,5,6,7] within and as part of the design process [8,9,10]. Further, the increasing ability to apply big data analysis tools to the data generated creates further issues in areas such as privacy [11]. While significant attention has been given over time to the 'hard' issues associated with ensuring data security through mechanisms such as those set out in Table 2, in general, less consideration has been given to the 'softer' or people oriented aspects of individual privacy.

In relation to 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. Consequently, companies are changing their

business models with data and/or data integration services becoming more important than hardware. Indeed, in 2014, Microsoft CEO, Satya Nadella, in an email to all employees signalled a shift in focus from devices and services towards mobile systems and cloud data.

This 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.

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' [12] which identified the following major areas of impact upon society:

People and 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, Communications and Storage – The continued decline in the size and cost of computing and connectivity technologies is driving an exponential growth in the potential to access and 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.

The 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.

3. 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 [13,14,15,16], which are typically structured as suggested by Fig. 4.

In the context of mechatronics, the associated structural relationships can then be illustrated by Fig. 5 from which it can be seen that mechatronics sits at the operational level of the procedural element, that of machine based systems. This suggests that therefore 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. This transfer must also include all necessary constraints related to the data and associated information, as for instance those related to privacy, both individual and global, issues.

The translation and interpretation of this data and information and it moves between 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).

Structurally, this has elements in common with the subsumption architecture as defined by Brooks in which behaviour is devolved downwards in a layered architecture of hierarchically organised sub-behaviours, each of which implements a particular level of behavioural competence. Higher levels then integrate or "*subsume*" these lower levels behaviours to create the overall system behaviour [17].

In the context of Figs 4 & 5, this means that system intelligence is distributed throughout the system form the mechatronics layer(s) to the cloud, with each layer functioning to provide its own specific behavioural contributions within an overall system context.
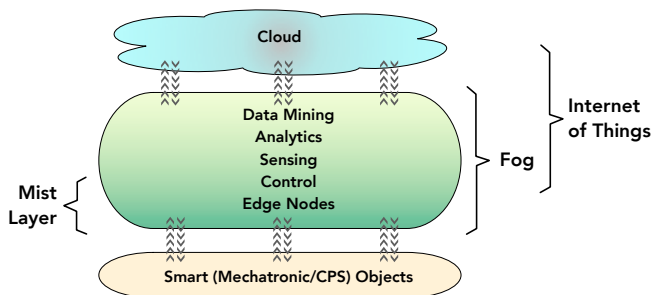

Fig. 6. Mechatronics, The Fog & The Cloud

3.1 Fog Computing

These relationships have led to the development of the concept of Fog Computing, defined by the National Institute of Standards and Technology (NIST) in the US as [18]:

> "… *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.*"

and embodying the relationships of Fig. 6.

Features of Fog Computing then include [18,19,20,21,22]:

Distribution – Supports highly distributed services.

Cloud to Things - Fog nodes are positioned close to the functional smart objects so that analysis and response times are reduced when compared than to a dispersed and distributed cloud.

Horizontal Architecture – Supports multiple application domains.

Interoperability - Seamless service support requires the co-operation of different providers which implies both interoperability and the federation of services across domains.

Mobility - Many Fog applications will be directly associated with mobile devices.

Real-Time Functionality – Support for the analysis in real-time of streamed data.

Sensor Networks – For instance as would be associated with the operation of a Smart Grid and including real-time validation and verification.

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. In the context of Fig. 6, the initial transfer, translation and interpretation is likely to form a part of the Mist Layer, and especially the edge nodes.

4. PRIVACY ISSUES

The interrelationships between the Internet of Things and Big Data raises significant issues of privacy and has resulted in the development by the Information & Privacy Commissioner of Ontario of the concept of Privacy by Design [23] in which control over and management of personal data is transferred to the individual.

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 [24,25,26], with a significant risk of impacting on the privacy of individuals [27]. 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* [28] 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

Table 3. Distribution of eHealth system activities

Area	Notes
People	An eHealth system provides support for individuals, or groups of individuals, in living independently through the provision of support based around biometric and activity monitoring.
Data	While the data associated with a single individual is directly and specifically related to the wellbeing of that individual, aggregated data over large numbers of individuals can be used both to identify trends and outcomes, and improve the interpretation of individual specific data.
Mechatronics	Mechatronic systems and sub-systems are responsible for the collection and distribution of source data.
CPS	The home environment can be considered as forming a cyber-physical system structured around an individual's personal wellbeing and encompassing factors such as comfort and environmental control.
IoT	The IoT provides both the connectivity between the individual and the wider network as well providing the mechanisms for feedback to the individual and the recalibration and resetting of their systems based on analysis of aggregated data.
The Cloud	Provides access to the necessary Big Data analysis tools used to assess and evaluate aggregated data.

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*' [11,29,30,31,32] 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 [11] 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 [32]:

- 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 [33]. 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.
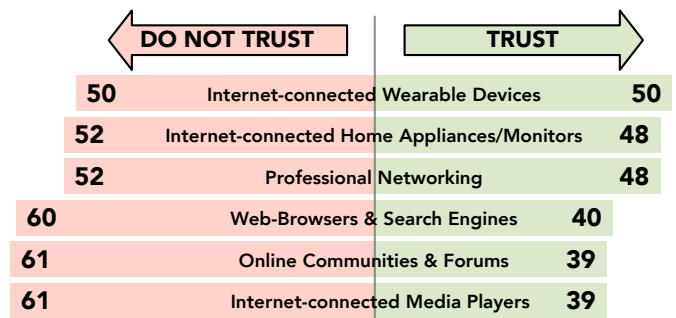

DO NOT TRUST		TRUST	
50	Internet-connected Wearable Devices	50
52	Internet-connected Home Appliances/Monitors	48
52	Professional Networking	48
60	Web-Browsers & Search Engines	40
61	Online Communities & Forums	39
61	Internet-connected Media Players	39

Fig. 7. Percentage of individuals trusting a technology, site or service {after [34]}

4.1 Public Confidence

Studies by the World Economic Forum [34] 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. In this context, Fig. 7 shows the results of a survey on the levels of trust that users assign to a range of features, with none achieving a trust level above 50%.

Figure 8 then shows user responses to questions as to how their levels of trust could be increased with respect to the way in which their persona data is managed at the level of the system. Here, the leading areas for change are associated with the ways in which their 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 system designers to have consider privacy issues from the very beginning of the design process.
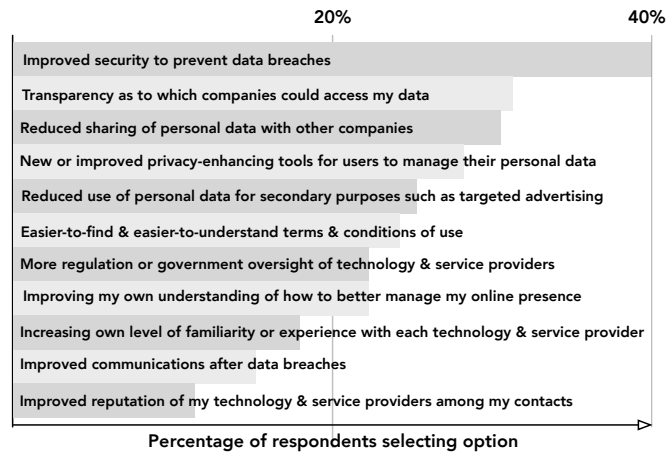

Fig. 8. User perception of changes intended to improve trust of technologies and service providers {after [34]}

5. eHEALTH EXEMPLAR

Consider the schematic of an eHealth system shown in Fig. 9 along with the functional distribution related to the aspects of People, Data, Mechatronics, CPS, the IoT and the Cloud as described by Table 3. The aim is to detect behavioural and related changes indicative of a change of status in the monitored individual and to respond accordingly [35]. The system inputs at the level of the user would typically be derived from a suite of environmental and behavioural sensors along with associated and appropriate biometric sensors and would include mobile (mHealth) sensors such as activity monitors [36,37] with a future potential for implantable sensors [38].

In the model considered, the individual specific source data would first be subject to analysis within their home environment to support short term responses to specific events such as falls. Only agreed and relevant behaviour related information would then be passed on to the care provider where it would be used to inform and modify the individual's care plan and electronic health record appropriately. Individually data would be held in the electronic health record with privacy protection incorporated at the level of the individual.

However, working at the level of the individual often means it is the case that changes can only be made retrospectively; i.e.
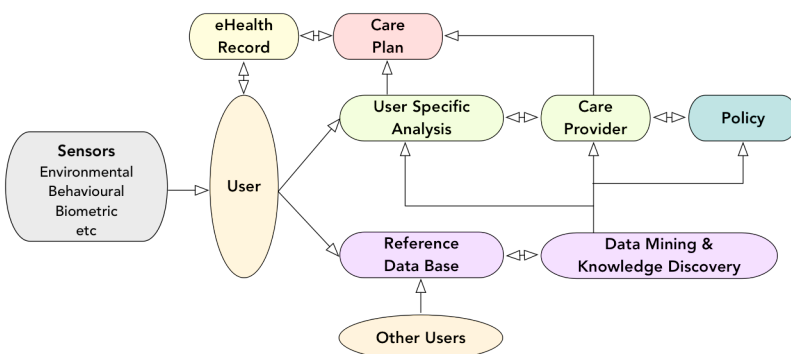
after an incident has occurred, as individuals are not in general presently considered as members of a much larger 0data community connected by and through the IoT. By integrating data across and between large numbers of individuals, and utilising data mining and knowledge discovery as applied to Big Data, additional knowledge can be established which can then be propagated to all individuals to enhance the user specific analysis for that individual. This however introduces additional questions of privacy in that data is now being aggregated across large numbers of individuals to support enhanced responses across all monitored individuals.

There is also a potential further requirement to release user specific information in relation to specific health related situations. For instance, in the case of an accident, responders are unable to target treatment if they are unaware of the patient's medical status including their current treatment profile. Similarly, emergency units are restricted in their capability until the patient's medical records are available. This suggests a requirement for a secure access procedure which does not rely on the patient being able to authorise and validate such access but which still ensures privacy.

This implies that knowledge about individuals, even when they are not of themselves specifically identified within the data set, is in danger of being revealed by a process of inference across the reference data set, something which relates back to issues of anonymisation of data and digital discrimination.

This then leads to questions as to how to design into the system appropriate protection for individual privacy while recognising the availability of a resource of much wider potential benefit, and how then to best exploit that resource for the benefit of the individual?

6. REVISING DESIGN METHODS AND PROCESSES

Based on the foregoing, the following key issues can be identified as being associated with a revision of mechatronics design methods and processes to accommodate the demands of both the IoT and The Cloud:

- Privacy issues and concepts must be embedded within the design from the beginning and not treated as an add-on.
- Specific privacy issues must be identified at the start of the design process so protected data is never accessible without the permission of the owner of that data.
- Interface requirements must be defined and the nature of the data transfer established early in the design process.

Fig. 9. eHealth system schematic and the associated functional distribution
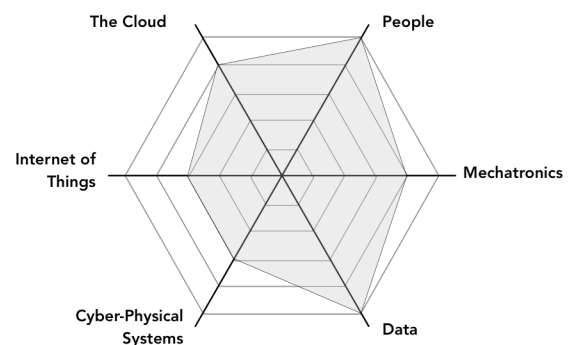
- The role of the user in specifying the functioning of the system needs to be better understood while ensuring the transparency of the technology to the user.

Taken together, the above suggest that the main modification to the design process is in the conceptual definition and idea generation phases of the overall design process rather than in the detailing phases. Referring again to Figs 4 & 5, this first implies that at the point of data capture the user can specify the level(s) of privacy to be associated with the generated data, thus defining the limitations on its access and use, while level of The Fog, itself a Process Layer in the context of Fig. 4, there needs to be some form of *Privacy Buffer* in which these privacy constraints are applied before the further upward translation of the data. From the perspective of the mechatronic system designer this requires the identification of such data for which there are privacy issues and for which the user must be able to set the level(s) of privacy to be associated with that data as suggested by Fig. 10.
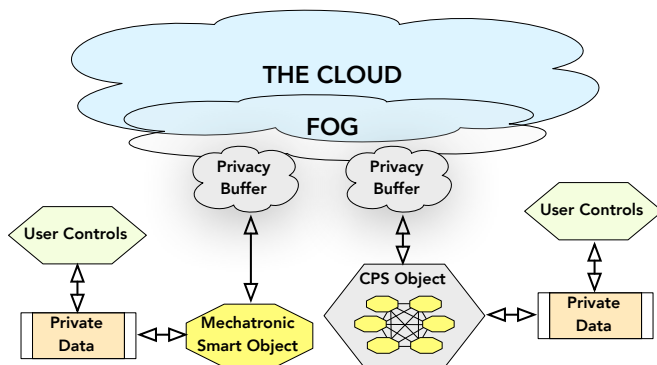

Fig. 10. Conceptualised data transfer model incorporating user control over private data and a privacy buffer

Following from the definition, identification, establishment and encoding of privacy issues within the designed context of the system structure, it is essential to ensure that all individual system elements have embedded within them the requisite capacity and intelligence to ensure that data integrity and privacy is maintained whilst supporting all necessary connectivity and transparency.

Based on strategic approaches to design structured around requirements analysis this implies the introduction of a function or feature-based approach to concept development in relation to the conceptualised data transfer model of Fig. 10 as follows:

Requirements - Identifies all potential privacy issues and their relationships with system operation. In the case of eHealth sensors, this would be associated with the collection, verification, validation and onward transmission of data. This in turn implies identification of both the source and destination of the data.

Specifications - Defines how data is to be handled in relation to individual privacy issues.

Concept Development - Establishes how the data is handled to meet the requirements of user privacy.

Data Validation & Verification – With the increasing deployment of distributed wireless networks there is a need to incorporate means for validating and verifying the derived data, particularly in relation to personal data and privacy issues [39,40].

Such a function based approach is not of itself new, and such representations to support concept development were under consideration over 20 years ago [41]. However, at the time they proved to be non-viable as the necessary processing power, and hence computer-based intelligence, to support the underlying decision making processes was not available, something which is no longer the case. Similarly, the modelling and descriptive design support tools now available can effectively facilitate and support the translation from a functional representation into a realisable form.

What is still required however is the development of underlying intelligent designer support methods and tools focused on the identification and mitigation of privacy related issues.

7. CONCLUSIONS

The paper has looked at some of the challenges facing a mechatronics oriented design team 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 concerns in relation to the interaction between such systems. Specific concerns over the ability to utilise data from multiple sources to enhance the ability to provide an effective response in areas are identified, with the case of eHealth being used as an exemplar of some of these. Also identified are concerns over the ability of design innovators working with evolving technologies to meet the requirements of future privacy oriented legislation.

In this context, a modification to the conceptual design process using a function-based approach is suggested as a means of supporting the identification of points of interaction between Cloud-based functions and other system components to support the integration of the precepts of privacy by design within the overall structure of engineering design throughout the conceptual design stages of the design process.

What is also clear is that many current mechatronic design guides [42,43] are lacking in any significant reference to privacy issues, and that this needs to be remedied [44].

REFERENCES

[1] Bradley DA, Mechatronics: More questions than answers, *Mechatronics*, *20(8),* 827–84, 2010

[2] Bradley DA, Russell D, Ferguson I, Isaacs J & White R, The Internet of Things – The Future or the end of Mechatronics, *Mechatronics, 27*, 57-74, 2015

[3] Schaar P, Privacy by Design, *Identity in the Information Society*, *3(2),* 267-274, 2010

[4] Cavoukian A, Taylor S & Abrams ME, Privacy by Design: Essential for organizational accountability and strong business practices, *Identity in the Information Society*, *3(2),* 405-413, 2010

[5] Radomirovic S, Towards a Model for Security and Privacy in the Internet of Things, *Proc. 1st Intl. Workshop on Security of the Internet of Things*, Tokyo, 2010

[6] Weber RH, Internet of Things – New security and privacy challenges *Computer Law & Security Review*, *26*, 23–30, 2010

[7] British Standards Institute, PAS 185:2017 Smart Cities – Specification for establishing and implementing a security-minded approach, BSI, 2017

[8] Roman R, Jianying Zhou & Lopez J, On the features and challenges of security and privacy in distributed internet of things, *Computer Networks*, *57*, 2266–2279, 2013

[9] Hui Suo, Jiafu Wan, Caifeng Zou & Jianqi Liu, Security in the Internet of Things: A Review, *Proc. Intl. Conf. Comp. Sci. & Electronics Engineering*, (ICCSEE), 648-651, 2012

[10] Qi Jing, AV Vasilakos, Jiafu Wan, Jingwei Lu & Dechao Qiu, Security of the Internet of Things: perspectives and challenges, *Wireless Networks*, *20*, 2481–2501, 2014

[11] O'Neill C, Weapons of Math Destruction, Penguin, 2017

[12] World Economic Forum Report Survey Report, *Deep Shift - Technology Tipping Points and Societal Impact*, WEF, 2015, @ www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (accessed 20 December 2017)

[13] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M & Ayyash M, Internet of things: A survey on enabling technologies, protocols, and applications, *IEEE Communications Surveys & Tutorials*, *17(4)*, 2347-2376, 2015

[14] 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, 2016

[15] Weyrich M & Ebert C, Reference architectures for the Internet of Things, *IEEE Software*, *33(1)*, 112-116, 2016

[16] Yang Z, Yue Y, Yang Y, Peng Y, Wang X & Liu W, Study and application on the architecture and key technologies for IoT, *IEEE Intl. Conf. Multimedia Technology*, 747-751, 2011

[17] Brooks R, A robust layered control system for a mobile robot. *IEEE J. Robotics & Automation*, *2(1)*, 14-23, 1986

[18] Iorga M, Feldman L, Barton R, Martin MJ, Goren N & Mahmoudi C, *The NIST Definition of Fog Computing*, NIST Special Publication 800-191 (Draft), August 2017

[19] Datta SK, Bonnet C & Haerri J, Fog Computing architecture to enable consumer centric Internet of Things services, *IEEE Intl. Symp. Consumer Electronics (ISCE)*, 1-2, 2015

[20] Yi S, Li C & Li Q, A survey of fog computing: concepts, applications and issues, *Proc. 2015 Workshop on Mobile Big Data*, 37-42, 2015

[21] Gupta H, Vahid Dastjerdi A, Ghosh SK & Buyya R, 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, 2017

[22] Munir A, Kansakar P & Khan SU, IFCIoT: integrated fog cloud IoT architectural paradigm for future internet of things *IEEE Consumer Electronics*, July, 2017

[23] Cavoukian A, *Personal Data Ecosystem (PDE)–A Privacy by Design Approach to an Individual's Pursuit of Radical Control*, Digital Enlightenment Yearbook 2013: The Value of Personal Data, 89-101, 2013

[24] Kambatla K, Kollias G, Kumar V & Grama A, Trends in big data analytics, *J. Parallel & Distributed Computing*, *74(7)*, 2561-2573, 2014

[25] Hsinchun Chen, Chiang RHL & Storey VC, Business Intelligence & Analytics: From Big Data to Big Impact, *MIS Quarterly*, *36(4)*, 1165-1188, 2012

[26] Raghupathi W & Raghupathi V, Big data analytics in healthcare: promise and potential, *Health Information Science and Systems (Online)*, *2(3)*, 2014

[27] Lazer D, Kennedy R, King G & Vespignani A, The Parable of Google Flu: Traps in Big Data Analysis, *Science*, *343*, 1203-1205, 2014

[28] Panniello U, Tuzhilin A & Gorgoglione M, Comparing context aware recommender systems in terms of accuracy and diversity, *User Modelling & User-Adapted Interaction*, *24(1)*, 35-65, 2012

[29] Kroll JA, Barocas S, Felten EW, Reidenberg JR, Robinson DG & Yu H, Accountable algorithms, *U. Pa. Law. Review*, *165*, 633-705, 2016

[30] Kim PT, Auditing Algorithms for Discrimination. *U. Pa Law Review Online*, *166(1)*, 189 - 203, 2017

[31] Danks D & London AJ, Algorithmic bias in autonomous systems, *Proc. 26th Intl. Joint Conf. on Artificial Intelligence*, 4691-4697, 2017

[32] Goodman BW & Flaxman S, EU regulations on algorithmic decision-making and a "right to explanation". *ICML Workshop Human Interpretability in Machine Learning,* New York, 26-30, 2016

[33] Landau S, Control use of Data to Protect Privacy, *Science - Special issue The End of Privacy*, *347(6221)*, 504-506, 2015

[34] World Economic Forum White Paper, *Shaping the Future Implications of Digital Me*dia for Society - Valuing Personal Data and Rebuilding Trust, WEF, 2017 @ www3.weforum.org/docs/WEF_End_User_Perspective_on_Digital_Media_Survey_Summary_2017.pdf (accessed 20 December 2017

[35] Brownsell S, Bradley D, Cardinaux F & Hawley M, Developing a Systems and Informatics Based Approach to Lifestyle Monitoring within eHealth: Part I - Technology and Data Management, *Proc. 1st IEEE Intl. Conf. Healthcare Informatics, Imaging and Systems Biology (HISB)*, San Jose, 264-271, 2011

[36] Ni Zhu et al, Bridging eHealth and the Internet of Things: The SPHERE Project, *IEEE Intelligent Systems*, 39-46, 2015

[37] Huan-Chao Keh et al, Integrating Unified Communications and Internet of mHealth Things with Micro Wireless Physiological Sensors, *J. Applied Sci. & Engineering*, *17(3)*, 319-328, 2014

[38] Darwish A & Hassanien AE, Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring, *Sensors*, *11(6)*, 5561-5595, 2011

[39] Henry MP & Clarke DW, 1993. The self-validating sensor: rationale, definitions and examples, *Control Engineering Practice*, *1(4)*, 585-610, 1993

[40] Benzaid C, Lounis K, Al-Nemrat A, Badache N & Alazab M, 2016. Fast authentication in wireless sensor networks, *Future Generation Computer Systems*, *55*, 362-375, 2016

[41] Bradley DA, Bracewell RH & Chaplin RV, Engineering Design & Mechatronics: The Schemebuilder project, *Res. Eng. Des.*, *4*, 241-248, 1993

[42] VDI 2206 Design methodology for mechatronic systems @ www.vdi.eu/uploads/tx_vdirili/pdf/9567281.pdf

[43] Gausemeier J & Moehringer S, New Guidline for VDI 2206 – A flexible proicedure model for the design of Mechatronic Systems, *Proc. 14th Intl. Conf. Engineering Design*, ICED 03, Stockholm, 785-790, 2003

[44] Zheng C, Hehenberger P, Le Duigou J, Bricogne M & Eynard B, Multidisciplinary design methodology for mechatronic systems based on interface model, *Res. Eng. Des.*, *28(3)*, 333-356, 2017