7th International Conference on Mass Customization and Personalization in Central Europe (MCP-CE 2016)

Mass Customization and Open Innovation
September 21-23, 2016, Novi Sad, Serbia

BUILDING ON THE EXPERIENCE OF SMART CITIES: ARE THEY SMART ENOUGH TO BE SAFE?

Maria Mikela Chatzimichailidou[1], Dusko Lukac[2]
[1]University of Cambridge, Cambridge, United Kingdom
[2]Rheinische Fachhochschule Cologne, Cologne, Germany

Abstract: *In this paper, the Internet of Things (IoT) is regarded as an ecosystem in which physical objects, human agents and dynamic relationships evolve. Those elements - affecting and affected by time and space - are jointly and self developed technologically and socially. Smart cities, as an application of the IoT, encompass technologies such as smart grids and intelligent transportation. Although their purpose is to improve public and personalised services, communication, quality of life and system sustainability, their safety is often disputed. A question that ought to be raised and answered in the near future is whether smart cities are smart enough to stand as a safe system, incorporating social and technical components. Safety concerns revolve mostly around automated transport systems and areas in which autonomous agents operate concurrently. This empirical position paper pursues to raise awareness on hidden hazards, and proposes three directions, which future research on IoT could take.*

Key Words: ***Accidents, Human Factors, Internet of Things, Safety, Smart Cities, Socio-technical systems***

1. INTRODUCTION

Acording to a generally accepted defintion [1], the Internet of Things (IoT) is a network of physical objects - devices, vehicles, buildings and other items - embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. In a similar manner, the GSMA Connected Living programme [2] links the IoT to the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects.

The building blocks of the IoT are connected devices, with a purpose to improve the quality of life of consumers. Consumers use wireless connectivity to enhance security systems, energy meters, household appliances, wearable devices, healthcare monitors and in-car experience. Thus, the IoT aims at creating value for and enhaning human environments, i.e. homes, retail environments, offices, factories, worksites, vehicles, cities, as well as outside environments [2].

In an effort to satisfy consumer needs, technology developers and manufacturers have been working on adding more intelligence and connectivity into objects [3], but without humans having to make any real effort or contribution to this accomplishment. However, in a world where consumers are more sophisticated than ever before and their roles are interchangable, the *'isolated consumer'* seems to be an illusion. Especially nowadays, not only does the consumer become an active player in the value-creating endeavour, he/she also becomes an entrepreneur and inventor. Therefore, a question that arises here is: *Should humans be thought of as passive users and/or consumers of technology?*

Along these lines, the paper in hand adopts a more holistic perspective and a systems view of the IoT. It suggests a shift in how we approach the concept of IoT. By way of explanation, the IoT can be seen as a field of integration between artifacts and humans, i.e. a socio-technical system. This research work adopts the definition that: *the IoT is an ecosystem in which physical objects, human agents and dynamic relationships evolve. Those elements - affecting and affected by conditions of time and space - are jointly and self developed both technologically and socially.*

To further elaborate on this perspective, Figure 1 offers a simplified schematic of the differences between the traditional IoT perspective and the one proposed herein.

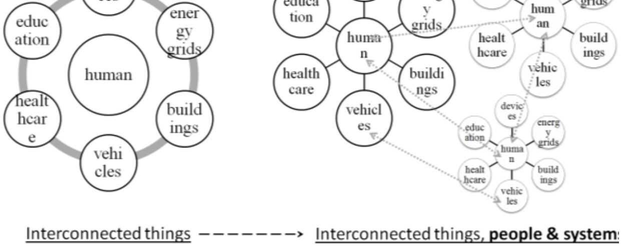

Fig.1. The traditional and the proposed perspective on the IoT

The authors perceive smart cities as a complex ecosystem, like the one depicted in Figure 1 (right). In both the left and the right network of Figure 1 the human component resides at the centre of the system, and interest as well. In the first case however (left), it is implied that the human factor is the constant in an ever-changing smart setting (see disconnected cicle in Figure 1). Technology revolves around the core, i.e. the human who makes use of the offered services, without however putting emphasis on his/her role as a co-creator or a determinant of the characteristics of the technology and the services being used.

According to the improved perspective, on the other hand, there are many humans who interact (see dashed arrows in Figure 1) with each other and with artifacts, and exhibit a dynamic behaviour. Moreover, in this second case, people and artifacts form systems, increasing (apparently) the complexity of the structure (see Figure 1), the range of system fuctions and processes, as well as the mechanisms that may cause disruptions to the normal operation of the system. The results of such a disruption may vary, for instance, in degree and reparability. As an example, they may refer to a mild disruption (e.g. a near miss that the system was able to handle owing to its resilience) or even to an accident, such as loss of human life, severe injury, property damage, environmental pollution etc.

Based on the above suggested IoT definition, this paper's objective is to raise the awareness of technology enthusiasts, and of the society in general, on the safety issues that may emerge in smart cities. This work presents some examples of hazardous technology and draws implications on the safety of smart cities and the vulnerabilities of the newly introduced, and sometimes immature, technology.

This is a position paper, that is a detailed written statement that articulates the authors' viewpoint about the safety issues within smart settings. The argumentation is based on the specialised know-how of one of the authors as a safety regulator and the experience of the other one on advanced technologies. This paper proposes three main directions, which future research on IoT could take. These directions are:

1. Go beyond an internet of things, notice and highlight the need for an integrated *internet of things and human factors* at the same time, i.e. humans are not just end-users of technology and services, but they also co-create and shape it according to their own needs and the platform they operate each time.

2. Smart cities are socio-technical systems; i.e. they do not comprise technology alone, but they form an ecosystem for technological as well as social innovation.

3. Smart cities, and smart settings in general, neither relate to safe processes axiomatically nor guarantee the safety of the human system components; it is not self-evident that smart cities are safer compared to the 'normal' ones. The many, and usually complex and latent, interactions between system components may trigger unwelcome situations, which are difficult to be perceived from the outset.

2. THE INTERNET-OF-THINGS CONTEXT

The IoT digitalises the physical world [4]. By blending physical and digital realms, it expands the reach of information technology. There is a myriad of possible innovations that arise from the ability to monitor and control things in the physical world electronically.

As mentioned previously, and according to the more traditional view, the IoT refers to the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects [2]. Moreover, it provides and strengthens the potential to fundamentally shift the way we interact with our surroundings. The ability to monitor and manage objects in the physical world electronically makes it possible to bring data-driven decision making to new realms of human activity; to optimise the performance of systems and processes, save time for people and businesses, and improve quality of life [4].

2.1. Internet-of-things applications in smart cities

So far, there is a great number of industry sectors that show significant adoption of IoT services. Figure 2 shows those categories.

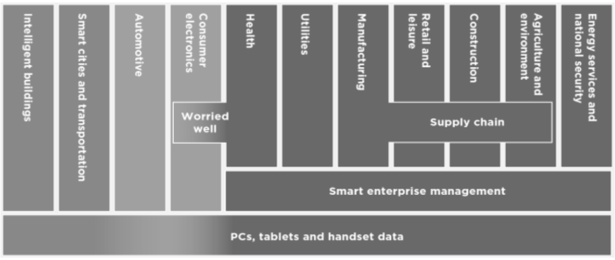
Intelligent buildings
Smart cities and transportation
Automotive
Consumer electronics
Health
Utilities
Manufacturing
Retail and leisure
Construction
Agriculture and environment
Energy services and national security
Worried well
Supply chain
Smart enterprise management
PCs, tablets and handset data

Fig.2. IoT Industry sector categories

Smart cities is one of the most discussed topics. Some examples of IoT applications in smart cities are given in Figure 3 [2]. They include smart streetlights to save energy, telematics to provide the drivers with real-time updates. It is also said that autonomous vehicles increase driver safety and reduce CO emissions. Smart traffic lights adjust the traffic in a dynamic way, while installed cameras enable faster first response assistance. Additionally, charges in the centres of big cities are determined by the behaviour of each driver.

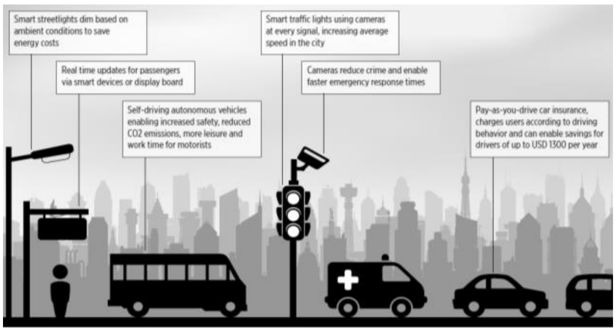
Smart streetlights dim based on ambient conditions to save energy costs
Real time updates for passengers via smart devices or display board
Self-driving autonomous vehicles enabling increased safety, reduced CO2 emissions, more leisure and work time for motorists
Smart traffic lights using cameras at every signal, increasing average speed in the city
Cameras reduce crime and enable faster emergency response times
Pay-as-you-drive car insurance, charges users according to driving behavior and can enable savings for drivers of up to USD 1300 per year

Fig.3. IoT applications in smart cities

Despite the wide applications of IoT services, this paper will only focus on smart cities since they are linked to implications for the safety of the people who use IoT services and interact with the urban ecosystem on an everyday basis.

3. SMART CITIES

A smart city is an urban development vision to integrate multiple information and communication technology (ICT) solutions in a secure fashion to manage a city's assets. Assets include, but are not limited to, local department information systems, schools, libraries, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services.

The goal of building and developing a smart city is to enhance quality of life by using technology to improve the efficiency of services and meet residents' needs. ICT allows city officials to interact directly with the community and the city infrastructure, and to monitor what is happening in the city, how the city is evolving, and how to enable a better quality of life. Through the use of sensors, integrated with real-time monitoring systems, data is collected from citizens and devices, then processed and analysed. The information and knowledge gathered are keys to tackling inefficiency [5].

3.1. Smart cities as socio-technical systems

Socio-technical systems comprise both 'socio', i.e. people and society, and 'technical', i.e. machines and technology, components. These components shape sub-systems that affect, and are affected by, the system's overall behaviour. For that reason, they have to be looked at as an entity. Furthermore, the parts of a complex socio-technical system are controlled by interconnected human or automated controllers/agents that possess reasoning mechanisms and demonstrate a capability to influence others or situations, in which they (may) find themselves [6].

Furthermore, smart cities are engineering systems, with a mission to be in service for people, offering them high quality as well as profitable services and infrastructure [6]. All in all, although smart cities have much to offer, accidents and/or incidents remain inevitable [6], notwithstanding how well-designed the engineered and/or the digitised part of the system may be.

3.2. Safety in smart cities

In the past, system designs were more intellectually manageable, and the potential interactions among components could be thoroughly planned, understood, anticipated, and guarded against [7]. Nowadays, in the era of smart cities, the complexity of systems and the world in which humans operate has increased enormously. The old safety engineering techniques, which were based on a much simpler, analog world, are diminishing in their effectiveness as the cause of accidents changes [7].

The most common and traditional accident causality models assume that accidents are caused by component failure and that making system components highly reliable or planning for their failure will prevent accidents. While this assumption is true in the relatively simple electromechanical systems of the past, it is no longer true for the types of complex socio-technical systems we are building today [7]. The more technologically improved systems become, the more critical the need for effective engineering approaches to improving safety and better managing risk.

In modern complex systems, accidents often result from interactions among components that all satisfy their individual requirements [7]. Practically, this means that although components do not fail, component interaction accidents are becoming more common as the complexity of system designs and operations increases.

As a result, causality needs to be extended to handle today's engineered systems. In a similar manner, the safety of smart cities cannot be assessed and dealt with using existent tools and mindsets. Designers and engineers have to consider smart ecosystems in their entirety, rather than just studying individual objects, such as electronics, software, sensors, and network connectivity. Human factors and their behaviour, (individual or coordinated) is also something that should not be disregarded.

In smart cities, humans are not just observers or machine-activators. They are integral parts of the system, they co-create their environment, stimulate the system states, and select the items they use, giving them at the same time specific characteristics and functions. Hence, building safe systems within smart cities requires integrating system safety, reliability and human factors into the basic system engineering process.

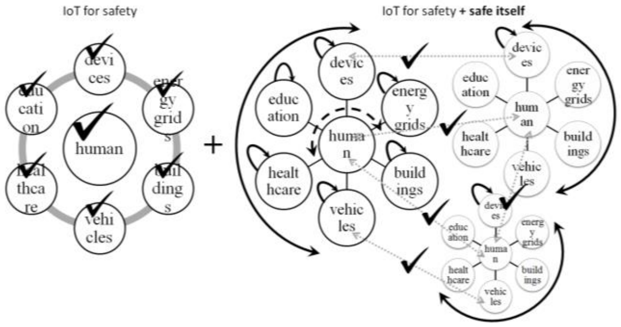

Fig.4. The traditional and the proposed perspective on the safety in smart settings

Figure 4 illustrates safety from a systems view. In the first half of the figure, safety concerns only the individual components of the system, without checking whether their in-between communication channels may be involved in an accident scenario. The first half of the figure is considered important but does not suffice to achieve system safety objectives. Besides, according to the traditional approach to the IoT, a smart city guarantees a safer setting compered to the common ones, like those we live in today. It is also said that smart cities can model safe cities [8]. All these imply that a smart city does not necessarily need to be subject to a safety assessment, because safety and security are embeded in smart cities by default. However, this is an assumption that requires some justification.

Based on the accidents and incidents reported so far in the literature, this paper puts the previous claim in question. Namely, it suggests a recursive and self-reflective assessment (see Figure 4, closed loop arrows) of the safety levels of the system as a whole, of its sub-systems, as well as of the reability of each system component. The communication channels between the system components, along with the corresponding interactions, should also be assessed on the grounds that they may probably impact on safety.

3.3. Frequent types of accidents in smart settings

In many reports, it is argued that IoT technology can prevent accidents. In [4] it is estimated that by using IoT there will be an overall accident reduction of 40% accident. It is also pointed out that if unmanned vehicles become fully autonomous (i.e. human operator decommissioned, but still an observer), then the accident reduction will reach 90%.

Although numbers like the above ones foster a positive predisposition towards the IoT technology, their estimate seems not to be founded on a solid systems or safety engineering theory. That is: *What kind of analysis was used to come up with the percentages? Was the analysis structured? From which point of view were estimates made? Were the analysis and the estimates safety-, technology- or budget-oriented?* These are only some of the questions that safety engineers, designers and technology developers should raise when rethinking how vulnerable, or even dangerous, a smart city may turn out to be.

Smart cities, although having as a purpose to improve public and personalised services, communication, quality of life and system sustainability, the safety they provide is frequently deceptive. Safety concerns revolve mostly around automated transport systems, e.g. unmanned vehicles, and areas in which autonomous agents operate concurrently and communicate. There is, for instance, a plethora of accidents and incidents that involve unmanned vehicles, either cars or drones, with the most recent being the Tesla crash[1]. There are also reservations about how unhackable IoT networks are. For that reason, Table 1 presents the results of a Google search made using the combination of the keywords given in the first row and the first column of the table.

Table 1. *Google search numerical results per keyword*

"AND" condition	"Driverless"	"Autonomous"	"Self-driving"
"Accident"	476,000	9,420,000	496,000
"Incident"	381,000	1,050,000	547,000
Retrieved on July *09, 2016*			

As a supplement to Table 1, Table 2 lists some of the near misses, accidents and reservations reported in the Press and involve autonomous and automated technology.

Table 2. *Articles in the Press about safety impricactions*

Title of article	Description
1. Drone Crashes, Hits 11-Month-Old Girl On The Head (Los Angeles Times)	Falling drone, loss of control
2. Google patents 'sticky car' to reduce crash injuries (BBC News)	Vehicle-human collision
3. That drone you want for Christmas will likely need to be registered (Los Angeles Times)	Security implications
5. Google driverless car crash was 'not a surprise' - A. Foxx, US transport Secreary (Independent)	Software fault; misunderstanding of the situation
6. Hacking into homes: 'Smart home' security flaws found in popular system (Michigan news)	Retrieve pin codes
7. This map lets you watch DDoS (denial-of-service) attacks in real time (The Daily Dot)	Unavailable machines or networks
8. The Amazon Dash Button Fiasco (PCMagazine)	Typical idealism
9. When Smart Cities are Stupid (International Newtown Institute)	Marketing material
10. Smart or stupid: will our cities of the future be easier to hack? (The Guardian)	Cyber attacks

Gathering all these examples together (see Table 1 and Table 2), a critical mass of arguments is built. These arguments are in favour of the *main claim* made in this paper that *despite the rapid technological developments of the IoT, safety is not yet fully studied and adequately considered*.

4. DISCUSSION AND CONCLUSION

The paper in hand, in comparison to the prevailing approaches, adopted a more holistic and systemic view of the IoT, highlighting the need for an integrated *internet of things and human factors* as well. Under this prism, smart cities were considered as complex socio-technical systems, rather than testbeds for technology research and development alone. In addition to that, the core of this position paper was the safety of smart cities, and smart settings in general, because they involve intense human activity.

So the question is: *Are smart cites smart enough to be safe?* The icreasing reliance on autonomous and unmanned operations, as well as on any other kind of sophisticated smart technology, is increasing the importance of other aspects of human-system interaction in the case of accidents [9].

By and large, it is undoubted that future, if not contemporary, cities will gradually become smart enough to sense human needs and preferences, before they even become explicit, and translate them into applications. The great *challenge*, though, would be to *built and develop them in such a way so as to be smart in terms of human/public safety*.

This heavy responsibility rests on the shoulders of engineers, designers and technology developers, along with the humans who operate systems in a smart city setting. Namely, they shall consider and carefully select the system elements and their characteristics, which can provide for the safety of the entire system, rather than waiting for accidents to happen and before the system suffers the consequences of an unwelcome situation. But more importantly, interactions among components should be thoroughly planned, understood, anticipated and guarded against.

As a plain example, let us assume that the objective is to assess the safety of a semi-autonomous vehicle. Evidence that it meets the minimun technical standards

[1] http://www.scientificamerican.com/article/deadly-tesla-crash-exposes-confusion-over-automated-driving/

alone seems to be insufficient for the assessment of the total safety of the system. But alongside with that, the human operator has to be skilled and certified, to comply with operation, maintenance and safety requirements, be able to and capable of operating in a platform where loads of incoming and outgoing data and information have to be managed. Moreover, the manufacturer should publish user manuals, while the responsible authorities should publish requirements. Things become even more complex when there are more than one semi-autonomous vehicles, and thus operators, within the same region and in close vicinity. In this case, vehicles and operators have to cooperate and coordinate their operations, so as to avoid collisions, deadlocks and other coordination and safety problems.

All in all, a smart city is more than the sum of its components [6], meaning that there is the *'something more' system element that emerges from the interactions between its components*. Bearing this in mind, the objective of this work was to raise the awareness of those who develop and use engagement and co-creation platforms to some sources of hazards associated with the complex and latent interactions between the system components.

So far, accidents in complex socio-technical systems (e.g. see Table 2) show that such hazards have triggered adverse events, which are difficult to be perceived from the outset. In sum, this work pointed to the potentially hazardous circumstances that draw implications on the safety of smart cities and the vulnerabilities of the newly introduced, and sometimes immature, technology.

To conclude, this paper anticipates the necessity to allocate future research attention on the system-wide and safety issues discussed in this piece of research. Moreover, if we wait for 'lessons learnt', then it may be too late as accidents occur. Thus, what is needed more is a proactive approach to managing technologies, humans, interactions, changes and, last but not least, systems safety.

Although security and privacy go beyond the scope of this study, future work can focus on addressing the related concerns raised. Further work can build the foundations for taking measures to protect privacy, accountability and transparency [10]. Moreover, it should be ensured that IoT technologies (e.g. unmanned aerial vehicles) pose the least amount of public risk and no threat to national security [10].

5. REFERENCES

[1] *Internet of Things Global Standards Initiative*, ITU, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[2] *Understanding the Internet of Things*, GSMA Connected Living Programme, http://www.gsma.com/connectedliving/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf

[3] *GSMA: The Impact of the Internet of Things The Connected Home*, GSMA Connected Living Programme, http://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf

[4] *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey & Company, http://www.mckinsey.com/global-themes/internet-of-things.

[5] S. Musa, *Smart City Roadmap*. Maryland, USA: University of Maryland, 2016, https://www.academia.edu/21181336/Smart_City_Roadmap.

[6] M. M. Chatzimichailidou, *RiskSOAP: a Methodology for Measuring Systems' Capability of Being Self-Aware of Their Threats and Vulnerabilities*. PhD Thesis, Athens, Greece: National Documentation Centre, 2016, http://www.openarchives.gr/view/2706282.

[7] N. Leveson, *Engineering a Safer World*. Boston, USA: MIT Press, 2011.

[8] L. G. Anthopoulos, “Understanding the Smart City Domain,” in *Transforming City Governments for Successful Smart Cities*, 2015, pp. 9–21.

[9] C. Johnson, “The Hidden Human Factors in Unmanned Aerial Vehicles,” in *International Systems Safety Society Conference*, 2008.

[10] *Operation and Certification of Small Unmanned Aircraft Systems*, Federal Aviation Administration, https://www.gpo.gov/fdsys/pkg/FR-2015-02-23/pdf/2015-03544.pdf

CORRESPONDENCE

Dr Maria Mikela Chatzimichailidou
University of Cambridge
Engineering Design Centre,
Trumpington Street,
CB2 1PZ Cambridge, UK
mmc60@cam.ac.uk

Dr Dusko Lukac
Rheinische Fachhochschule
Robotics and CAD Lab/ University-Industry Cooperation,
Vogelsanger Str. 295
50825 Cologne, Germany
dusko.lukac@rfh-koeln.de