IoT Devices and Smart Buildings:

Starting on the Right Foot

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Andrew Villca-Rocha

Spring 2021

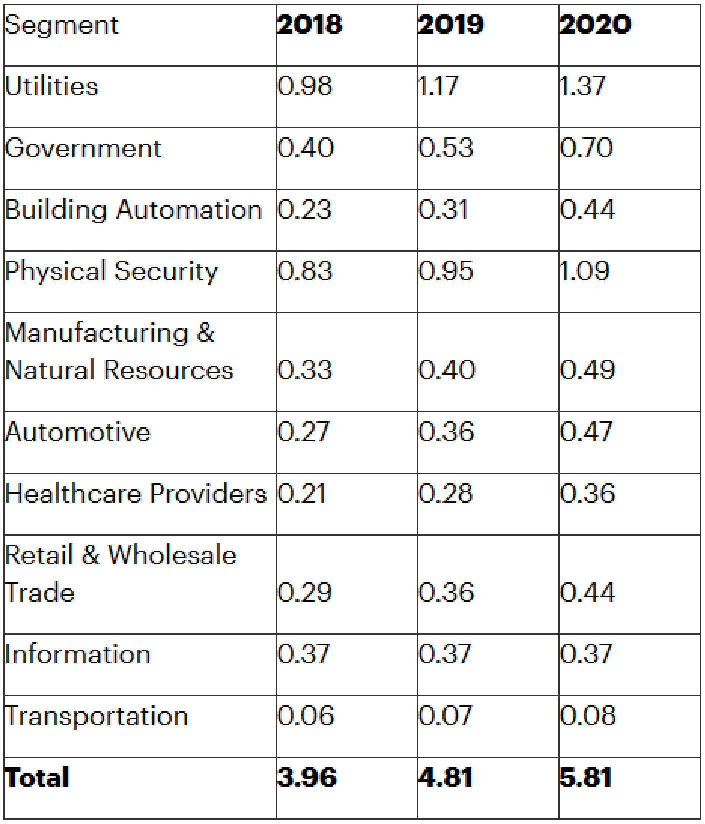
On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

IoT, Internet of Things, devices are one of the byproducts of the explosion of the internet. IoT devices are a term that references pieces of hardware, such as sensors, appliances, or machines, that can transmit data over the internet or other networks. Nowadays many devices around us at every given minute are connected to the Internet in some manner (Goasduff, 2019). Furthermore, previously disconnected machinery within buildings are getting connected to the internet. As seen by Figure 1, this trend crosses all industries. These IoT devices are often used as "sensors" to gather data from the real-world. One example of this are smart buildings. These are buildings that utilize IoT devices to increase efficiency (Flax, 1991). This increase in efficiency through the use of IoT devices can bring efficiency benefits, but at what cost?



Segment	**2018**	**2019**	**2020**
Utilities	0.98	1.17	1.37
Government	0.40	0.53	0.70
Building Automation	0.23	0.31	0.44
Physical Security	0.83	0.95	1.09
Manufacturing & Natural Resources	0.33	0.40	0.49
Automotive	0.27	0.36	0.47
Healthcare Providers	0.21	0.28	0.36
Retail & Wholesale Trade	0.29	0.36	0.44
Information	0.37	0.37	0.37
Transportation	0.06	0.07	0.08
Total	**3.96**	**4.81**	**5.81**

Source: Gartner (August 2019)

Figure 1: Table shows the growing IoT Endpoint Worldwide Market (Billions of Units) by Industry from 2018-2020. (Goasduff, 2019)

As IoT devices continue to grow in use, it remains unclear how this will affect user's trust, safety, and relationships with previously trusted technology, specifically buildings. IoT devices transform buildings into smart buildings capable of increasing efficiency. However, as IoT devices are used more and more it does not necessarily guarantee their safety (Shwartz, 2020). Having more data rich information can attract bad actors who wish to maliciously invade user's privacy and safety. Because of this uncertainty in the security of IoT devices there is potential for an unwanted change in how users interact with buildings. Previous research has shown that user's trust and willingness to use technology relies on their perceived security risk (Vosooghi, 2019). If the security of buildings is tarnished by the introduction of IoT devices, then this could damage the current relationship users have with buildings. People may avoid smart buildings if they deem it unsafe which in turn could lead to the failure of institutions (businesses, schools, offices, etc). Therefore, reversing any advancements in the use of IoT devices to increase efficiency.

In this paper, I argue that significant attention must be placed on the infrastructure of smart buildings in order to ensure successful use of IoT devices. I believe that it is important to analyze the problems that IoT devices introduce to smart buildings; otherwise, users would not be able to take advantage of the benefits IoT devices bring. In order to accomplish this, I utilized documents discussing the overarching trend, Industry 4.0. IoT and smart buildings are a part of Industry 4.0; therefore, insight specific to our use case can be drawn from these documents. Because IoT devices are being used by the entire market, I believe that it is important to place ethical responsibility upon the individual user who should consciously choose how to use IoT devices rather than remaining complacent and treating the extensive deployment of IoT devices as inevitable.

Problem Definition

In the past decade, IoT devices have experienced a steady 20% increase in use every year. They are becoming prevalent in many industries like the government, building automation, manufacturing & natural resources (Goasduff, 2019). These devices are able to gather massive amounts of data that can be analyzed for valuable information and provide a perspective of the real world. One such example is smart buildings.

Smart buildings are buildings that incorporate IoT devices into their infrastructure to achieve some efficiency. These buildings can use sensors like occupancy sensors to adjust their temperature based on how many people are present in a given room. Essentially, these IoT devices provide an oracle (building manager) a view into the state of a building which allows them to make efficiency-oriented decisions. Managers strive for efficient decisions because it saves the owner money and, possibly more important, it can lead to environmentally conscious decisions (Flax, 1991). However, the use of IoT devices doesn’t only introduce positive effects.

The increase in use of IoT devices also introduces some uncertainty in the security of the technologies. For instance, smart cars incorporate IoT devices into their cars in order to provide navigation and self-driving capabilities. However, it has been found that because cars are now connected to the Internet it is susceptible to malicious actors who could steal driver’s metadata or even hijack the control of the car itself (Kunkle, 2019). In recent years, researchers have discovered that introducing IoT devices to previously secure technologies also introduces security vulnerabilities (Gilchrist, 2017). This is because old technologies are steadily getting connected to the internet. “Exceptionally, no network is free from security threats and vulnerabilities”, in cybersecurity anything connected to the internet must be assumed to be vulnerable to malicious actors (Hu, 2016). What this entails is that technologies previously thought of as secure will be considered insecure as it incorporates IoT devices into its infrastructure. But this not only affects smart buildings but also the trend it is a part of.

I4.0 is an overarching global movement towards ushering the industry into the "next industrial revolution". This new industrial revolution seeks to fully connect systems in order to create fast data flow and automation of processes. IoT devices are used in I4.0 to connect these systems to the network (Sartal, 2020). Because of this, I4.0 inherits the security ambiguity from the use of IoT devices.

The ambiguity around the use of IoT devices is rather alarming when placed within the context of Industry 4.0 (I4.0). I4.0 discussions have a language of inevitability. Epicor, a provider of I4.0 solutions, emphasizes in their article that I4.0 technology is needed in your business to provide a "sustainable, scalable enterprise in today's business environment" (Epicor, 2021). Although they are pushing a product, there is a sense of FOMO (fear of missing out) if a business prefers to avoid I4.0. Additionally, academic discussions of I4.0 further push inevitableness. For instance, an article providing a survey on I4.0 states "Everyone should accept the fact that everything in the world is changing" when discussing the digital transformation I4.0 brings (Sartal, 2020). Even simply relating I4.0 to historical industrial revolutions gives this movement a sense of "bigger than us" while ignoring the negative consequences that can arise. A combination of inevitableness towards I4.0 and security flaws introduced by IoT devices stresses the importance for a design-oriented discourse that gives people the power to change the course of inevitability.

What I wish to accomplish with this STS research paper is to analyze current research into I4.0 and the challenges it faces translating them to IoT devices and smart buildings. Pulling these challenges down to a more focused context may help with easing feelings of inevitability.

Methods

In order to identify the challenges that face IoT devices and smart buildings, I analyze the literature available for I4.0. Significant progress has already been made by I4.0 researchers in analyzing the state of its progress and the challenges it faces in the future. One such document that I analyzed was Enabling Technologies for the Successful Deployment of Industry 4.0. This document will be referenced as ETSDI from now on.

ETSDI is a book with chapters written by different I4.0 experts from different universities across Europe. The chapters were then edited together by researchers and professors from the University of Vigo and the University of Aveiro. As stated in the Preface, this book's objective is to "provide an accurate and clear vision about what [I4.0] consists of, explaining its purpose, the challenges to overcome, and, above all, a detailed description of the various technologies that integrate it and its applications." They also state that this book is meant for specialists and non-specialists. Thus, giving us insight into the current language used to engage with the general public about I4.0. Lastly, they focus on organizational and technological sides of the industries employing I4.0 giving us proper insight into the sociotechnical functioning of I4.0.

The second source I selected for analysis is Is Industry 4.0 a Good Fit for High Performance Work Systems?. authored by Todd D. Rutherford and Lorenzo Frangi. Is Industry 4.0 a Good Fit? is an article from the Relations Industrielles journal from Quebec, Canada that covers industrial relations. The article covers a study of UNIFOR union locals in Canadian automotive assembly plants. They argue that I4.0 must be analyzed similarly to the ways unions have influenced the universal adoption of HPWS, a new high performance work system. From this they stress the importance of the worker's role in negotiating the integration of I4.0 because of its path-altering transitions for employment relations. This work was selected for its unique insight into the people rather than the technology when it comes to implementing I4.0.

I will be analyzing the relevant evidence within the guidance of Neeley and Lugenbiehl's Beyond Inevitability: Emphasizing the Role of Intention and Ethical Responsibility in Engineering Design. In Beyond Inevitability, the authors focus on the impact of our way of speaking about the process of the introduction of technology in society. They argue that current discourse on emerging technologies conveys a sense of inevitability. They describe this sense of inevitability as simply a chain of developments where human actors can only add another link without changing previous iterations. Instead, they find it more beneficial to view technological development as "an opportunity for the expression of creative and original impulses". One way they suggest accomplishing this is by utilizing language of design rather than that of technological development. They demonstrate this by contrasting inevitable language like "General Trend" with more design oriented languages like "Specific Innovation", "Progress" with "Change", and "Team" with "Individual". With this in mind, I hope to make an effort towards maintaining a discourse of design rather than a discourse of technological development.

Using Beyond Inevitability as a framework works hand in hand with discourse regarding IoT devices and smart buildings. I4.0 suffers from inevitability. As discussed previously, businesses like Epicor utilize marketing tactics to push I4.0 with language that convey FOMO to potential customers. Additionally, language in ETSDI attempts to convince readers of the importance of I4.0 by stating things like "..., everything is changing. There is no way to stop this.". Since IoT devices and smart buildings are a part of the general I4.0 trend, discourse surrounding these topics inherently suffer from inevitability. I am deviating from the "General Trend" (I4.0) in favor of a more *specific* focus on IoT devices and smart buildings. Therefore, I am presented with an opportunity to ensure the discourse surrounding IoT devices and smart buildings deviate from the technological development language found in I4.0 marketing and ETSDI.

Results

I will now begin to discuss some important information extracted from my research and then discuss inferences we can make about IoT devices and smart buildings. *ETSDI* dedicates each chapter towards a subsection of I4.0. Chapter 1 focuses on digital transformation, a main catalyst towards I4.0. Digital transformation is defined as the changes associated with digital technology applications and integration of that to all aspects of human life. IoT devices help digital transformation because of its ability to digitize and infuse with the existing technology around us. From this discussion on digital transformation, the authors identify challenges facing various industries as they incorporate digital transformation into their business model to facilitate I4.0.

Of these challenges I have selected a few that I believe can be translated into ones that are relevant to smart buildings. Firstly, "The digital designers should place a lot of effort in finding solutions to the problems without stopping the manufacturing lines". This is with regards to developing smart systems within smart factories. But, the idea can be translated to smart buildings. Implementing IoT devices in such a way that disrupts the current operating functionality of the building will require a redesign of the entire operation behind said building. Secondly, connectivity and security must be valued. Since IoT devices' main function is to gather and transmit information, it is vital for the network infrastructure of the building to be able to sustain the heavy traffic. A failure in the network could result in a failure in the operation of the entire building. Additionally, security must be emphasized to protect the extensive and sensitive communication amongst IoT devices. Since these devices are important to the efficient functioning of the building, emphasis must be placed on the integrity of these systems. Finally, I4.0 implementation is complex and thus relies on interdisciplinary expertise. Smart buildings also ensure this complexity. For instance, hardware (IoT devices) is designed to integrate with the building's current technology, network specialists setup network connections across the building and ensure its security, AI solutions are invented to gather inferences from the data given by IoT devices, and software engineers create the software to allow humans to interact with this data. Therefore, a variety of professionals are needed in order to implement and maintain smart buildings.

Chapter 5 of ETSDI, introduces cloud computing as a solution for offloading the cost and challenges of implementing and maintaining I4.0. They claim that businesses that do not have access to the needed expertise can contract other entities to implement I4.0 for them. However, this solution still introduces problems. For instance, this does not solve the needed network robustness and security within the smart building. This is true because in order to utilize a cloud computing solution the building needs to transmit the data over the internet to the cloud computing business rather than maintaining all the data within the building. So in some regard this is even more unsafe. Furthermore, diverse IT expertise is still needed within the building in order to maintain the systems communication with the cloud computing service. Additionally, cloud computing services seem affordable since you won't have to worry about server costs and software but catering to a specific building's needs can increase the costs. Cloud computing at its current iteration does not solve the challenges introduced by Chapter 1.

Returning to Chapter 1 of ETSDI, the author places importance on the human aspect of the implementation of I4.0. Even though I4.0 through digital transformation is intended to replace traditionally human roles with autonomous ones, people remain the main driver for the processes. When a role has been automated there is still a need for human intervention in the form of directions to the autonomous process. Therefore, people will remain a key actor in the transition towards I4.0. Smart buildings see a similar relationship with building managers. Ideally smart buildings would limit the need for building managers but, as the technology progresses, they are needed more than ever to provide human intelligence to the system.

Is Industry 4.0 a Good Fit? shares this thesis in their analysis of worker unions in Canadian automotive industries. Their findings showed that unions and firms will have little overlapping interests in I4.0. Therefore, they suggest workers to maintain a strong “monopoly face” in order to retain leverage in an evolving workplace. Cooperation amongst firms and workers will be harder due to the lack of shared interests. They stress “keeping workers at the centre of decision-making when it comes to technological change in the workplace” (Rutherford, 2020). Using this information, we gain insight into how the evolving workplace from I4.0 can damage the relationship between firms and workers. This further stresses the importance of human actors in the transition towards smart buildings.

Using the information gathered from I4.0 documents, I suggest significant attention must be placed on the infrastructure to ensure the successful use of IoT devices in smart buildings. This infrastructure can be categorized into three groups: network, human, and economic. Smart buildings derive their efficiency from IoT sensor data therefore the network infrastructure must be robust enough to support this data flow. Furthermore, the network must be secure to prevent data leaks and any malicious action that could jeopardize the operation of the smart building. Humans also play a big role in the implementation of I4.0 and they too play a role when implementing IoT devices for smart buildings. Therefore, an infrastructure should support the people that work within the smart building. Whether this be education for current employees to get accustomed to the new technology and the efficiencies it brings or hiring the right people to manage and implement the systems within the smart buildings. Placing importance in the people may help alleviate the lack of shared interests warned in Is Industry 4.0 a Good Fit?. In order to support the previous two groups of infrastructure, significant economic infrastructure must be emphasized in the initial design of the smart building. The firms must acknowledge that in order to properly support a smart building's infrastructure there should be available capital for investments into the smart building. This may require significant innovation and imagination from firms or governing bodies.

Without a focus on the infrastructure of smart buildings, then the project would be doomed to fail. Ignoring the importance of the network early in the design process will make future modifications more complicated and more expensive. Failing to place importance into the people within a smart building will leave the system void of human intelligence and cooperation, which emerging I4.0 technology needs to be able to take advantage of IoT sensor data. Additionally, placing importance into the people of smart buildings brings issues closer to their control. These people will be the ones engaging in imaginative solutions for problems that may arise in smart buildings. If the goal is to see widespread implementation of smart buildings then infrastructure needs to be in the initial design discussions of the project.

Conclusion

Analyzing current research into I4.0 and the challenges it faces reveals that focusing on the design of the infrastructure for smart buildings is vital for successful implementation because the network infrastructure is vital for the usage of IoT devices, which in turn is vital for the efficiencies smart buildings bring. Additionally, the human infrastructure of a smart building is just as important. Investing into the human infrastructure of a smart building places more focus on the people and thus creating more opportunities for creative solutions. Lastly, in order to support the other two types of infrastructure, economic infrastructure needs to be established.

By recognizing the types of infrastructure that should be focused on, I have steered people towards better focusing their design plans when implementing IoT devices in smart buildings. Additionally, I have refrained from using language of inevitability and instead focused on utilizing design language to put more emphasis on the individual, thus giving implementers more responsibility when choosing to advance towards I4.0.

There are a few limitations to the research I conducted. First, my research fails to address the issue of inevitability with the language surrounding I4.0. This scope is much larger and requires someone to create a compelling narrative that is rooted in engineering principles. Second, my research isn't as exhaustive as I hoped it would be. There is more information that can be used to build on the insights I brought forth in my research. For instance, delving into other I4.0 technologies besides smart buildings may bring other new insights not blatantly seen in smart buildings. Lastly, my research simply recognizes that the infrastructure of smart buildings is a point of focus. I never introduce a practical plan for implementing the correct infrastructure.

References

Claval, P. (1988). European rural societies and landscapes, and the challenge of urbanization and industrialization in the nineteenth and twentieth centuries. *Geografiska Annaler. Series B, Human Geography, 70*(1), 27. doi:10.2307/490739

Deloitte. 2018. “IoT Innovation Report.” https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Internet-of-Things-Innovation-Report-2018-Deloitte.pdf.

Flax, B.M. (1991, April 1). Intelligent buildings. *IEEE Communications Magazine, Communications Magazine, IEEE, IEEE Commun. Mag*, 29(4), 24 - 27.

Gilchrist, A. (2017). *Iot security issues*. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy01.its.virginia.edu

Goasduff, L. (2019, August 29). Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020.

Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020. Gartner. (n.d.). https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io.

HU, F. (2020). *SECURITY AND PRIVACY IN INTERNET OF THINGS (IOTS): Models, algorithms, and implementations*. S.l.: CRC PRESS.

Kunkle, F. (2019, April 20). Auto industry says cybersecurity is a significant concern as cars become more automated. *The Washington Post*. Retrieved from https://www.washingtonpost.com/transportation/2019/04/30/auto-industry-says-cybersecurity-is-significant-concern-cars-become-more-automated/?noredirect=on

Rutherford, T. D., & Frangi, L. (2020). Is industry 4.0 a good fit for high performance Work Systems? Trade unions and workplace change in the Southern Ontario automotive Assembly Sector. *Relations Industrielles, 75*(4), 751. doi:10.7202/1074563ar

Sartal, A., Carou, D., & Davim, J. P. (2020). *Enabling technologies for the successful deployment of industry 4.0*. Boca Raton: CRC Press.

Venturini, T. (2010). Diving in magma: how to explore controversies with actor-network theory. Public Understanding of Science, 19(3), 258–273. https://doi.org/10.1177/0963662509102694

Vosooghi, R., Kamel, J., Puchinger, J., Leblond, V., & Jankovic, M. (2019, December 1). Robo-Taxi Service Fleet Sizing: Assessing the Impact of User Trust and Willingness-To-Use. *TRANSPORTATION,* 46(6), 1997 - 2015.