The Future of Aviation: Integrating IoT in The Aerospace Industry

Nicole G. Kutcher[1]
University of Tennessee, Knoxville, Tennessee

This paper reviews the upbringing of the Internet of Things (IoT) and its integration into the aerospace industry. IoT has the ability to enhance aircraft operations, maintenance, system dependability, and energy and environmental efficiency. Implementation requires a unique skill set that bridges a gap between engineers and Information Technology (IT) professionals, highlighting the necessity of educational systems that incorporate key facets of each expertise. This paper calls attention to potential hazards and threats that IoT may pose to high-tech systems. To advance IoT in aerospace, it is critical to mitigate costly cybersecurity risks through the utilization of strict frameworks and continued study of the topic. In all, this paper acknowledges the current weight of IoT among developing technology and the future opportunities it presents to the aerospace community.

I. Nomenclature

CIoT = *Consumer Internet of Things*
IIoT = *Industrial Internet of Things*
IoT = *Internet of Things*
IT = *Information Technology*
OT = *Operational Technology*

II. Introduction

In 1999, the term "IoT" was first coined by a British technologist, Kevin Ashton [1]. The Internet of Things (IoT) is a network that "bridges the cyber domain to everything and anything within [the] physical world" [2]. Essentially, IoT connects physical devices, appliances, and other objects so that each of them can collect and exchange data. This process includes the embedment of multiple sensors and other detectors to extract data and relay it to differing systems.

Within the last two decades, IoT has developed in many different directions. Its subsets include Consumer Internet of Things (CIoT), Commercial Internet of Things, Industrial Internet of Things (IIoT), Infrastructure Internet of Things, Internet of Military Things, as well as various others [4]. Each of these comprises varying types of devices for altering purposes. CIoT includes devices such as smartphones, smart assistants, home appliances, and wearables that focus on short-range communication in homes and offices. Commercial IoT delves further into the idea of CIoT and projects similar goals onto larger venues like supermarkets, stores, hotels, healthcare facilities, and more [4].

The most well-known form of IoT is IIoT which focuses on implementing IoT in industrial systems and factories. This process is typically much more complex and advanced than the two previous subcategories. Figure 1 illustrates the complexity of IoT implementation in industrial processes. Infrastructure IoT technically is a subset of IIoT, however its significance allows it to be treated as a separate category. Specifically, Infrastructure IoT implements smart infrastructures–both urban and rural– that incorporate IoT in order to boost efficiency, cost savings, and maintenance. Lastly, the Internet of Military Things applies IoT to military and battlefield circumstances. This

[1] Undergraduate Student, University of Tennessee Knoxville, AIAA Member, 1810922.

subcategory is aimed at “increasing situation awareness, bolstering risk assessment, and improving response times” [4]. Other categories that include IoT involvement are the medical field, health and fitness, agriculture, and more.

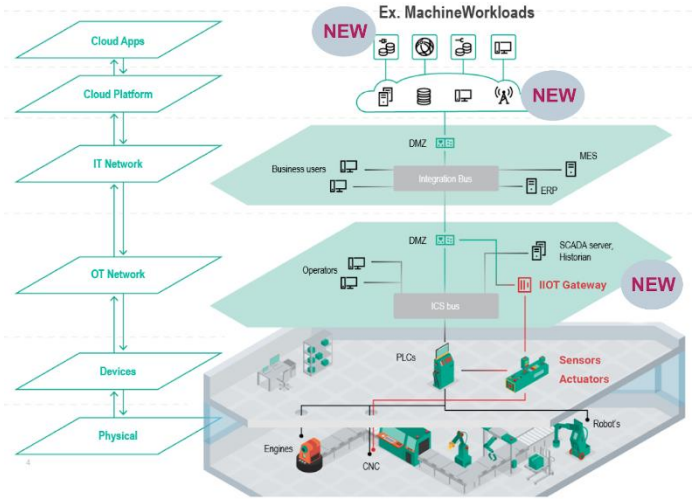

Fig. 1. Illustration of a factory infrastructure that implements IIoT [3].

Given these subcategories, it is evident that IoT is being implemented in every aspect of societal development. Researchers around the world predict that IoT will be the next industrial revolution due to the potential that the network holds [5]. More so, it is believed that IoT will be the “building block” for this upcoming revolution and “smart-world era” [2]. Many of these predictions have been foreseen through the presence of smart homes and wearable health devices. Even so, advancements are growing at an exponential rate, and future applications are much closer than many believe.

III. IoT in the Aerospace Sector

IoT has the ability to record and analyze complex data more timely and efficiently than humans. Additionally, its technologies are able to enhance control and monitoring over production which is a critical step in manufacturing and performance processes [5]. Consequently, IoT is becoming increasingly prominent in various industries, including the aerospace industry.

Advancements guide insights without parallel in several aspects of aircraft operations. Aircraft health has been carefully examined so that IoT technology can identify possible challenges and make proactive maintenance approaches in early stages [6]. These preventative measures help avoid catastrophic accidents, waste of resources and funds, and loss of time in high-pressure circumstances. More so, through enhanced maintenance predictability, engineers have made progress in minimizing operational downtime, improving system dependability, and streamlining maintenance timetables [5]. Aviation technologies require precise, high-quality engineering to ensure optimal safety for passengers. Given this, IoT advancements have already paved a path towards a more consistent and safe future.

In other aspects, IoT is also aiding airlines to make progress in their passenger experience. The integration of IoT has allowed many airlines to create more personalized environments for passengers. Airbus, the largest aeronautics and space company in Europe and a leading aerospace company across the globe, has specifically highlighted their involvement with IoT as a way to express the value they have for their passengers. The company has shared the launching of the “Connected Experience” solution. Through this, the cabin crew has access to digital services to support passengers and data is taken during and after the flight that provides insight into passenger behavior [7]. The goal of this application is to improve cabin flexibility and service in the future for all customers. Evidently, IoT has become involved in industrial and commercial aspects of the aerospace industry and is prompting growth in both aspects.

IV. Risks Pertaining to IoT

Despite the many advantages and benefits of IoT, there are considerably just as many concerns. Figure 2 illustrates various challenges that arise from the integration of IoT in the aerospace industry. Many concerns pertain to the security of IoT technologies. IoT deals with a great amount of data, and in doing so, puts the data in a vulnerable

position. Security and privacy threats can undermine entire companies. More importantly, security breaches, threats, and identity attacks can hinder global economies and demographic issues as well [8]. Put differently, exposing vast amounts of data poses a great threat to entire companies and industries. As a result, this concerns any organizations that interact with the original company and can create a cascading effect of damage.

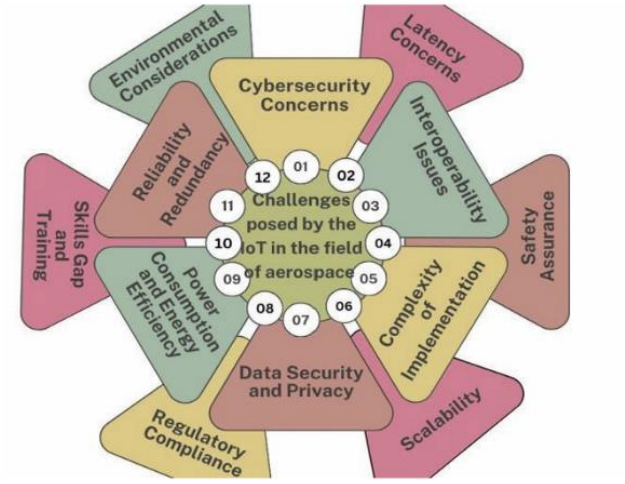

Fig. 2. Challenges resulting from the integration of IoT in the aerospace field [10].

Attacks can transpire in various ways. One of which is a routing attack. Data can be forwarded and information be transmitted in order to accumulate perceptual information [1]. This version of attack would greatly impact systems that collect classified and confidential information. For example, if a foreign entity staged a routing attack on a government organization, like NASA, this could put the United States' scientific progress in an alarming position. Retrieving classified information could fuel identical discoveries in rival entities and allow for those entities to use the given information to infiltrate harm on NASA's systems. Another form of attack is a denial of service (DoS) attack. Much like the title implies, a DoS attack denies users authorized access by overwhelming the system with traffic [1]. Referring to the previous example, assume that a foreign entity disrupted NASA with a DoS attack. This would inhibit NASA from being able to continue research and place the organization in an unproductive and useless state.

Indeed, researchers published in the academic Journal of Cleaner Production that "protecting the systems and data from potential attacks are therefore mandatory" due to potential security risks [5]. It is indisputable that IoT data networks require strict protections in order to ensure the security and productivity of the systems. Closer examination also acknowledges that the aerospace industry contains much more military and classified government data that intensifies the extent of destruction that a security breach can provoke.

Likewise, other risks are brought up by the great amount of data that IoT systems run off. Concerns have been raised about whether or not resources can manage the amount of data. Specifically, in a study aimed at analyzing how satellite architecture can perform with IoT framework, researchers concluded that the huge amount of raw data contained by IoT technologies can stress the resources and network in correlation [9]. Despite the great improvements that IoT has contributed, if it is too advanced for many systems to coexist and collaborate with, then it will have no future for any industry.

Skill set also plays a factor in concerns with IoT. The maintenance of IoT is often overlooked because of its ability to process data without human intervention. However, like all networks, there must be some human interaction to ensure efficiency. In order to create IoT technologies, one has to understand the engineering technicalities behind the appliance and the Information Technology (IT) technicalities in order to master the design. This prompts a challenge considering that most people trained in IT don't have engineering expertise and vice versa. This phenomenon is also discussed in the International Journal of Intelligent Networks. Researchers declared that many industries have developed and managed IT, however Operational Technology (OT) is a completely different domain and developing both domains is much more difficult for industries [6]. While IT focuses on managing data, OT relies on controlling physical processes and equipment. Given this, IoT utilizes both types of technology to perform correctly and effectively. A problem therefore arises because many industries do not have the skillset or expertise to manage IoT technologies. This puts industries in a position where they must choose to withdraw the use of IoT technologies and essentially be behind those that do implement IoT in their work, or they can choose to

implement IoT without understanding the network to the full extent. This raises many more risks considering that industries don't truly understand what they are working with and may not perform the proper maintenance and guidelines to upkeep IoT technologies. If companies continue to apply IoT technologies in their work without having a full understanding of the network, then they will not be able to detect malfunctions or properly react in emergency situations.

When applying these concerns to the aerospace industry, the strict standards that require manufacturing to meet exact tolerances and safety must also be acknowledged. There is no room for error in the field and implementing IoT systems without completely understanding how to maintain and control them is not acceptable. As previously stated, work within the aerospace industry can contain classified information and implementing IoT technologies without fully understanding how to put security and privacy guards in place can lead to destructive exposure of intellectual property. There needs to be a greater understanding of the technology before its use is implemented throughout the entire industry.

V. The Future of IoT in Aerospace

As seen through many of the risks pertaining to the implementation of IoT in the aerospace industry, IoT application must be studied further. Research has identified specific aspects of IoT that should be focused on including better diagnostics, autonomous systems, and cybersecurity [10]. The security of IoT must be ensured from early stages of prototyping to the publication of its performance [1]. Close attention through every stage of the system's development will magnify its dependability and safety.

Furthermore, the sustainability of IoT applications must also be accounted for. This can attempt to resolve the issue surrounding resources and systems that cannot entirely support IoT technologies because research will identify what systems are most capable of coexisting and collaborating with IoT. Additionally, focus on sustainability can strive towards cost-effective materialization. IoT depends on wireless sensor nodes for short transmission ranges, limited energy supply, and constrained computational capabilities [11]. Prioritizing the cost-efficiency of these materials will expand IoT presence in all fields, especially aviation.

The next step in the IoT industrial revolution depends on the education of IoT in engineering. The complex data network requires a unique skill set that interconnects IT with data engineering. An obstacle surfaces as a result of this necessity: necessary educational programs. Very few educational institutions hold programs that allow a co-curricular education of IT and engineering that can appeal to IoT or IIoT technologies. An exemplary program that addresses these concerns is the Internet of Things/Interdisciplinary Engineering program at Purdue University. This Master of Science degree "emphasizes preparation for an industry career as a technical leader" [12]. Similarly, the Massachusetts Institute of Technology offers Professional Education courses that aim to teach concepts and applications of Industrial IoT [13]. Each of these programs focus on integrating IoT concepts with engineering technical applications so that individuals can develop the skills that IoT technology demands.

Introducing cutting-edge educational programs that teach the understanding and implementation of IoT in the industrial workforce is critical for the future of IoT. With time, as more programs become accessible nationwide, narrowing the focus of some of these programs will optimize the impact of IoT as well. More so, a program with an emphasis on IoT implementation in the aviation and aerospace industry will prepare engineers for industry-based work in this field.

VI. Conclusion

IoT has progressed quickly in the last two decades and many subsets of its foundational ideas have been inherited in various industries. The network provides great promise in the aerospace sector in relation to aircraft operations. Maintenance predictability has reduced the waste of materials, operational downtime, and increased the dependability of aerospace systems. IoT has integrated technology into commercial aviation and improved passenger experience and cabin crew service. Despite these advances, risks pertaining to security and privacy are present and growing. Even slight cyberattacks to IoT systems can cause detrimental effects to businesses, the government, and the entire economy. IoT is developing at a quick rate, perhaps quicker than engineers are able to keep up with. If integration into various industrial workforces is forced too early, destructive events may transpire and great amounts of data can be exposed or lost. If IoT continues to improve the efficiency and sustainability of aerospace manufacturing processes, preventative measures must be put in place to ensure the safety of information.

Acknowledgments

Thank you to Dr. Damiano Baccarella for his guidance and support in the writing of this paper. Thank you to Emma Elise Ferber for her mentorship and support as well.

References

[1] B. K. Tripathy and J. Anuradha, Eds., Internet of things (IoT): technologies, applications, challenges and solutions. Taylor & Francis, CRC Press, 2018.

[2] O. M. Bushnaq, A. Celik, H. Elsawy, M.-S. Alouini, and T. Y. Al-Naffouri, "Aeronautical Data Aggregation and Field Estimation in IoT Networks: Hovering and Traveling Time Dilemma of UAVs," IEEE Transactions on Wireless Communications, vol. 18, no. 10, pp. 4620–4635, 2019. doi: 10.1109/TWC.2019.2921955.

[3] "IIoT: Enabling Your Factory via Digitisation," Irish Manufacturing Research, Jun. 10, 2019. [Online]. Available: https://imr.ie/2019/06/10/project-industrial-internet-things-iiot/.

[4] "Internet of Things: The Five Types of IoT," Syntegra, Aug. 22, 2022. [Online]. Available: https://syntegra.net/internet-of-things-the-five-types-of-iot/.

[5] D. Rodrigues, P. Carvalho, S. Rito Lima, E. Lima, and N. V. Lopes, "An IoT platform for production monitoring in the aerospace manufacturing industry," Journal of Cleaner Production, vol. 368, p. 133264, 2022. doi: 10.1016/j.jclepro.2022.133264.

[6] D. L. Andersen, C. S. A. Ashbrook, and N. B. Karlborg, "Significance of big data analytics and the internet of things (IoT) aspects in industrial development, governance and sustainability," *International Journal of Intelligent Networks*, vol. 1, pp. 107–111, 2020. doi: 10.1016/j.ijin.2020.12.003.

[7] :IoT: Aerospace's Great New Connector," *Airbus*, Jul. 4, 2019. [Online]. Available: https://www.airbus.com/en/newsroom/stories/2019-07-iot-aerospaces-great-new-connector.

[8] G. K. Panda, B. K. Tripathy, M. K. Padhi, and J. Anuradha, "Evolution of Social IoT World: Security Issues and Research Challenges," in *Internet of Things (IoT)*, 1st ed., CRC Press, 2018, pp. 77–98. doi: 10.1201/9781315269849-5.

[9] M. Luglio, M. Marchese, F. Patrone, C. Roseti, and F. Zampognaro, "Performance Evaluation of a Satellite Communication-Based MEC Architecture for IoT Applications," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 5, pp. 3775–3785, 2022.

[10] R. Rajora, A. Rajora, B. Sharma, G. R. Kumar, P. Aggarwal, and S. Thapliyal, "Advancing Horizons: Exploring the Aerospace IoT Revolution - Analysis, Advancements, and Prospects for the Future," in *2024 3rd International Conference for Innovation in Technology (INOCON)*, pp. 1–5, 2024. doi: 10.1109/INOCON60754.2024.10512339.

[11] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[12] "Internet of Things/Interdisciplinary Engineering," Office of the Vice Provost for Graduate Students and Postdoctoral Scholars - Purdue University, 2022. [Online]. Available: https://www.purdue.edu/gradschool/prospective/gradrequirements/westlafayette/inot.html.

[13] "Online Course Industrial Internet of Things," MIT Professional Education, 2023. [Online]. Available: https://professionalprograms.mit.edu/online-program-internet-of-things/.

[14] J. Bernal and B. Sridhar, Industrial IoT for Architects and Engineers. PACKT Publishing Limited, 2023.