# Strengthening The Defence Industry's Independence Through The Internet Of Things In The Manufacturing Sector: A Review

Jonathan Ernest Sirait[1*], Hazen Alrasyid[2], Nadia Aurora Soraya[3]

[1,2,3] Faculty of Defence Technology, Indonesian Defence University, Indonesia
[*]Corresponding Author:
Email: jonathan.sirait@tp.idu.ac.id

***Abstract***.
*Digitalization is needed by manufacturing companies in organizing sustainable, data-driven, effective and efficient, safe defence and security equipment production activities. Utilization of Internet of Things (IoT) in Indonesia is said to still have many deficiencies, resulting in many cases of data leakage, both government and private sector data. The purpose of this research is to review the conditions of the use of the IoT in various industrial sectors, the challenges, and the potential for development in the Indonesian defence industry. A literature review approach is combined with a qualitative method in this study. The results of this study found that the application of IoT to Indonesia's defence industry is necessary in order to increase the level of local content, complement and strengthen defence and security equipment, and reduce the burden of production activities. In addition to production needs, IoT can filter information or data on weapons or combat vehicles when used in field tasks and then become the basis for making subsequent products.*

***Keywords:*** *Internet of Things, Smart Manufacture and Indonesian Defence Industry.*

## I. INTRODUCTION

The adoption of communication and information technology is growing rapidly every year with features that facilitate daily work. Not only used by individuals, many applications of information and communication technology have been applied to organizational activities, companies in various fields and sectors to accelerate business processes and gain maximum profit. Digital manufacturing can be defined as the digitization of the supply, production, and delivery operations of networked firms, and employs a digital model that is applied to operations intensively [7]. In the industrial era 4.0, the defence industry dominated by manufacturing companies is disruptively driven by the presence of information and communication technology. The demands of today's manufacturing industry are certainly very different compared to the early days of the Industrial Revolution. Modern production focuses not only on quantity or quality, but also on resource conservation and process sustainability [8]. In the midst of a world economy that is affected by political pressure, changes in natural conditions, technological developments accompanied by intense business competition - the manufacturing industry is also required to apply digitalization such as by implementing smart manufacturing or cloud computing so that it is able to compete and not be crushed by competition from other countries [14]. The product manufacturing, marketing, and after-sales processes can all be improved and monitored in real-time through digitalization, which also able to cut unnecessary costs and boost operating profits [15].The prospect of Indonesia becoming an IoT ecosystem is immense. This possibility can be seen from the number of active internet users in the country, which are more than 170 million people [4].

In essence, the transformation of Industry 4.0 is one of the key to the growth of Indonesia's development. So as the country is not only a market for the digital economy, but also takes advantage of the development of the digital economy in order that the industry can grow and be more competitive [22]. Moreover, in the repercussions of the Covid-19 pandemic which pushed back the world economy; on the other hand, it provides learning for industry players in utilizing technology to increase productivity. Conventional work systems have undergone several changes, such as increased automation, increased use of digital equipment, utilization of digital data and analytics, increasing tracking, the growth of various online platforms [18]. Utilization of IoT technology nowadays have been effectively took advantage in dissimiral industrial sectors for monitoring, surveillance, and remote decision making.As the defence industry is dominated by manufacturing companies, they are always trying to create a security defence equipment

product based on user modification requests. The TNI, Polri or the government as the main buyers for the defence industry adapt products to the spectrum of threats in every task related to national defence - security, then these needs will be met by the domestic defence industry through their products. In connection with Industry 4.0, manufacturing systems has been upgraded to an intelligent level. In order to address a dynamic and global market, intelligent manufacturing makes use of cutting-edge information and manufacturing technologies to gain flexible, intelligent, and reconfigurable manufacturing processes [20].

Therefore, the capabilities that the manufacturing industry needs to have in this era are called "Four Plus One (4+1)", namely the ability to improve production quality, speed up delivery times, capabilities in terms of low production costs, environmental eco-friendly products, and ultra-customization or ultra-personalization [14].The benefits of industrial IoT in terms of predictive maintenance, energy efficiency of each machine, demand forecasting, supply chain visibility [6], are inseparable for the domestic defence industry. The goal of independence of the defence industry is also inseparable from the application of the latest technology, both in the final product and the production process. This is also intended so that the fulfillment of national minimum basic forces can be met in the midst of increasingly complicated national and international dynamics. Defence industry companies that produce good quality defence and security equipment are closely related to the health of the upstream and downstream environment in which the products are made; in a sense, the industrial ecosystem greatly affects the results and quality of the products made, regardless of where the products are made [19].The Industrial Internet of Things (IIoT) and its application in the manufacturing sector present numerous opportunities to boost business value. The country's manufacturers will also be able to compete more effectively in the global economy if industry players digitize faster. This will certainly have a major impact on how to strengthen the resilience of Indonesia's economic foundations. The pandemic itself has helped accelerate digital technology adoption as businesses and individuals go about their business while avoiding person-to-person contact [2].

## II. METHODS

This research was carried out using a qualitative method with a literature review approach. Results and analysis are carried out by absorbing various literature such as books, journals, articles, news, online documents, the internet related to the research topic which are then extracted, filtered with the aim of evaluating information based on predetermined criteria.

## III. RESULT AND DISCUSSION

The Internet of Things (IoT) itself initially used the current internet infrastructure and existing technologies to turn stand-alone objects (i.e. devices) into interconnected smart objects [12]. The IoT is changing manufacturing for both suppliers and customers as it develops in the industry. The IoT connects the shop floor and back office to the digital world. For manufacturers, it is physical things like machines, tools, and the people who operate them which drive the production process and create the end-product. Then IoT then links these things and their domain to a network so that accurate information can be shared immediately. IoT applications in Indonesia have been used in a variety of industries, including the management of cities, agriculture, fisheries, and transportation. Due to the urgency of their needs and requirements, numerous business development collaborations, both government-to-business and business-to-business are becoming increasingly intense in various parts of Indonesia [11].As a country that has strategic resource wealth, Indonesia is expected to be able to meet its defence needs in a sustainable manner. However, the contribution of the domestic defence industry to the fulfillment of the minimum essential force (MEF) is still not optimal [5]; [1].The defence industry, which is influenced by political, technology, economic and social factors, has certainly faced the impact of the Covid-19 pandemic where the company's supply chain, business development efforts, export-import, finance and competence, stock prices are greatly affected and only a few companies can survive through this [21].

The time it takes for new information to translate into concrete action will shorten as digital disruption spreads, primarily through increased connectivity and technological capabilities. However, the supply chain becomes a dynamic, integrated supply network as each supply node becomes more capable and

connected. Because it adds value to various products through systems that apply cutting-edge technologies to conventional products in both manufacturing and services, smart manufacturing is regarded as a crucial perspective for the future in both research and application [24]. This means that its development in the defence industry is very broad. It is shown in Figure 1 where the company will be able to communicate quickly with users and production management can carry out production supported by interconnected production capabilities, the right suppliers, effective product development according to the dynamics in the field. As a result, a production management system needs fleet management, predictive maintenance, condition/status monitoring, the digital twin, data-driven research and development, and several production conditions in line with Industry 4.0 trends [3].

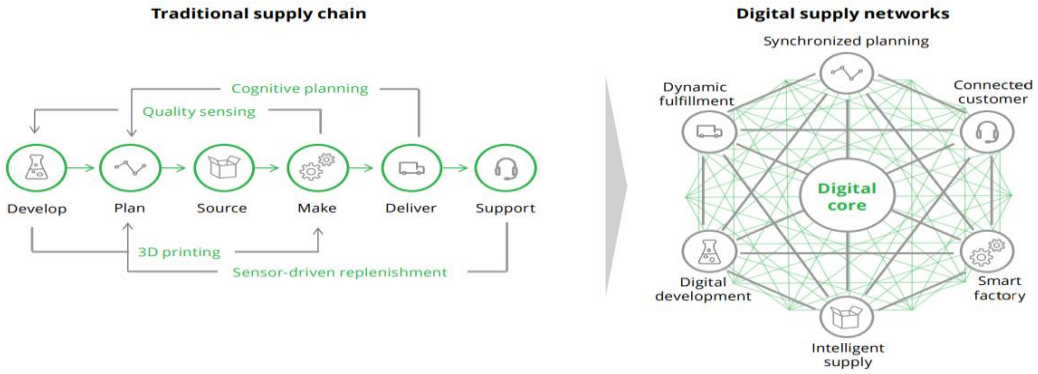


**Fig 1.**Traditional Supply Chain Shift To Digital Supply Network. Source: Deloitte (2016).

The key characteristics of IoT enabled manufacturing include: Smart manufacturing systems based on Auto-ID technology, Real-time data collection, Real-time visibility and traceability of production processes, Real-time manufacturing decision-making [24]. Furthermore, the application of IoT utilization for the manufacturing industry can be applied from the initial process of the company processing raw materials to monitoring after sales activities [13]. These includes production systems, human resources, supply chain sustainability, and product life-cycle. That way, defence industry companies that require supply connectivity from upstream industries network (Tier 3 and Tier 4) to downstream industries (Tier 1 and Tier 2) can maximize the level of local content (TKDN) in accordance with the national industrial vision and mission.

**Table 1.** Iot Potential For Defence - Security Equipment Needs. Source: Army Technology (2022)

| No. | Emerging | Accelerating | Maturing |
|---|---|---|---|
| 1 | Aircraft stowage ejectors | Remote-controlled pick-up drones | Assisted aiming guided by sensors |
| 2 | Remote-controlled drones | Remote-controlled drone imaging | Systems for aircraft flight control |
| 3 | Aircraft anti-collision systems | Multi-axis drone gimbals | Solar-powered UAVs |
| 4 | Aircraft powertrain control | Collapsible PV modules | |
| 5 | Remote-controlled pick-up drones | Drone launching techniques | |
| 6 | | Remote-controlled drone launchers | |
| 7 | | Aircraft power distribution network | |
| 8 | | UAV swarm control | |
| 9 | | Parachutes integrated with unmanned aircrafts | |
| 10 | | Battery thermal management system | |
| 11 | | Drone flight control system | |
| 12 | | Drone battery swapping | |
| 13 | | Lidar-Sonar fusion | |
| 14 | | Satellite image smoothing techniques | |
| 15 | | Lidar for vehicle anti-collision | |
| 16 | | Radar for vehicle anti-collision | |

Table 1 shows the potential development of IoT applications for the manufacturing industry/defence-security sector. As seen in Table 1 at a glance, it shows the significant potential of IoT that can be applied to land, air, and sea vehicles for the purposes of surveillance, monitoring, and maintenance systems. This is where the role of companies in the defence industry that specialize in electronic system integration, such as the state-owned PT Len Industri and a number of other private companies involved in this subfield, work

hand in hand to innovate and build an integrated weapon system with the use of IoT technology.By way of explanation, the presence of IoT is also needed in equipping and strengthening a weapon system product with a wealth of data when personnel perform tasks; including how companies provide the best quality in producing them. this is also related to the involvement of the Internet of Military Things (IoMT). IoMT applications play a major role in collecting various types of data such as equipment and vehicle fleet management, battle data (patterns, strategies, etc.), soldier's health monitoring, enemy identification, smart bases, remote training, data processing and analysis [10]. Integrating IoT into existing military and defence infrastructure can help troop mobilization become more efficient, effective and can significantly reduce casualties and equipment damage in combat. In addition, the data that has been collected after the battle can become the basis for defence industry companies and military to coordinate with each other to analyze and make product updates that are in accordance with real conditions in the combat area.

Simultaneously, the positive impact of using IoT in the manufacturing industry also allows various industry players to compete more competitively in niche markets and are required to produce more strategic product innovations. Various challenges in terms of managerial, systemic, business process, and security factors [3]; [16] are also a scourge that must be faced when the company's transformation towards digitalization is carried out.To support a sustainable production process with IoT, one of the obstacles still faced by the entire national industrial sector is data security. Referring to the Indonesian Defence Industry Law, which states that the implementation of the defence industry is based on the confidentiality principle. Naturally, not all of the production activities carried out by players in the defence industry are made for public. On the other hand, advances in technology that break down physical dimensions can make it possible to get information in a variety of different ways. The weak data security system in Indonesia is the cause of the increasing problem of data theft, where in 2020 to 2021 there were more than 450 million cases of data leakage [17]. From the brief explanation about regarding the IoT's advantages and positive effects, it is abundantly clear that IoT provides valuable information and data for enhancing the company's quality and competitiveness [23]. Because it is extensive in scope and interconnected at every stage, one of the most significant risks in Indonesia's defence industry ecosystem must be addressed throughout the IoT lifecycle process. Figure 2 depicts how IoT applications across a variety of industries and services interact with one another and how these industries can be targeted for data breaches.

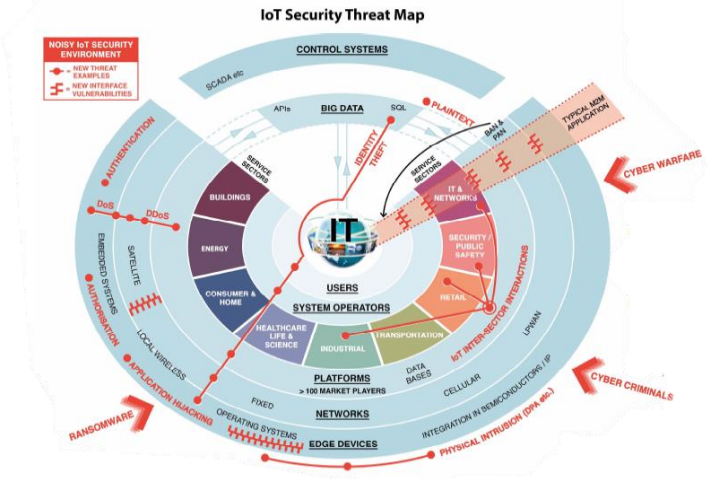


**Fig 2.** IoT Security Threat Map. Source: Beecham Research (2015)

The parliament approved the personal data protection law in October 2022. This is one of the government's positive steps in supporting industry players. In fact, there are still a lot of areas that can be improved to provide maximum protection, such as enhancing information and communication technology capabilities in company human resources and investing in IoT architecture and data leak mitigation systems with strong deterrence. Strengthening data security in IoT is simply directed at securing 3 IoT domains, namely the Cloud Domain which includes a number of servers that operate the entire data operation; Fog Domain which is a tool that connects various smart equipment; and Sensing Domain in the form of smart devices capable of sending data in real time to the Fog Domain [9].

## IV. CONCLUSION

Indonesians will continue to promote the use of IoT, with the various advantages offered by this paradigm as various regions in Indonesia continue to develop, with the need to solve industrial problems increasing over time. Indonesia's goal of strengthening and modernizing its defence industry is a long process that proceeds with continuity and no shortage of challenges, even as new opportunities are pursued. Human resources enriched with IoT capabilities need to be supported by the policies of industry players in accelerating the implementation of digitalization through IoT. Its benefits in increasing productivity, minimizing human error, data-based insights, efficiency and reducing operational costs are needed by defence industry companies to produce high-quality and highly competitive defence-security equipment. The vast opportunities of the national defence industry, supported by ready-to-use resources, have the potential to be utilized by the defence industry to support the productivity and export value of defence-security equipment at the global level. Accelerating the digitalization of the defence industry is important as one of the efforts considering the condition of Indonesia, which is recovering the economy after the pandemic.

## V. ACKNOWLEDGMENTS

The authors are grateful to the CNPq National Council of Scientific and Technologic Development for supporting this project, to the Center for Lasers and Applications' Multiuser Facility at IPEN-CNEN/SP and to Anton Paar Brasil for the use of the Raman spectrometer. We also thank Teodora Camargo and Tatiana Russo from the *Núcleo de Conservação e Restauro* in *Pinacoteca do Estado de São Paulo* for the invaluable advices.

## REFERENCES

[1] Aida, Ade Nurul. (2021). Potret Industri Pertahanan Indonesia. Retrieved from https://berkas.dpr.go.id/puskajianggaran/kajian/file/kajian-226.pdf, accessed on 5 January 2023.

[2] Agarwal, Rajat, Antonius Santoso, Khoon Tee Tan, Phillia Wibowo. (2021). Ten Ideas To Unlock Indonesia's Growth After COVID-19. Retrieved from https://www.mckinsey.com/featured-insights/asia-pacific/ten-ideas-to-unlock-indonesias-growth-after-covid-19, accessed on 5 January 2023.

[3] Albukhitan, Saeed. Developing Digital Transformation Strategy for Manufacturing, *Procedia Computer Science*, 2020, vol. 170. p. 664-671, doi: https://doi.org/10.1016/j.procs.2020.03.173.

[4] Badan Pusat Statistik (BPS). (2021). Indeks Pembangunan Teknologi Informasi dan Komunikasi 2021. Retrieved from https://www.bps.go.id/publication/2022/09/30/5fe4f0dbccd96d07098c78d3/indeks-pembangunan-teknologi-informasi-dan-komunikasi-2021.html#:~:text=IP%2DTIK%20Indonesia%20tahun%202021,59%20pada%20skala%200%E2%88%9210., accessed on 5 January 2023.

[5] Basundoro, Alfin Febrian. Kebijakan Minimum Essential Forces untuk Meningkatkan Kapabilitas Tentara Nasional Indonesia di Kawasan Indo-Pasifik. doi: 10.13140/RG.2.2.31849.93289, 2020.

[6] Bhagat, Varun. (2021). Digital Transformation in Manufacturing- A New Wave for the Industry [Benefits and Trends]. Retrieved from https://www.pixelcrayons.com/blog/digital-transformation-in-manufacturing-benefits-and-trends/#2_IIoT, accessed on 5 January 2023.

[7] Borangiu, Theodor, Damien Trentesaux, AndréThomas, PauloLeitão, Jose Barata. Digital Transformation Of Manufacturing Through Cloud Services And Resource Virtualization, *Computers in Industry*, 2019, vol. 108, p. 150-162, doi: https://doi.org/10.1016/j.compind.2019.01.006.

[8] CFI Team. (2022). Intelligent Manufacturing System (IMS). Retrieved from https://corporatefinanceinstitute.com/resources/valuation/intelligent-manufacturing-system-ims/, accessed on 29 December 2022.

[9] Dabbagh, Mehiar, Ammar Rayes. (2017). Internet of Things Security and Privacy, Retrieved from https://www.researchgate.net/publication/309375790_Internet_of_Things_Security_and_Privacy, accessed on 7 January 2023.

[10] Deepali. (2022). Applications of Internet of Things (IoT) in Defence and Military. Retrieved from https://www.naukri.com/learning/articles/applications-of-internet-of-things-iot-in-defence-and-military/, accessed on 6 January 2023.

[11] Hadiyana, Mochamad. (2019). Digital Inside: Ekosistem IoT di Indonesia # 1. Retrieved from https://www.youtube.com/watch?v=QsJFQKHdpic, accessed on 6 January 2023.

[12] Hassan, Qusay F. Internet of Things A to Z: Technologies and Applications. New Jersey: John Wiley & Sons, Inc. 2018.

[13] Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Shanay Rab, Rajiv Suman, Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT), *Sensors International*, vol. 2, p. 1-16, doi: https://doi.org/10.1016/j.sintl.2021.100129, 2021.

[14] Kiswanto, Gandjar. (2020). Indosat Business: Manfaat Menerapkan Teknologi IoT pada Industri Manufaktur. Retrieved from https://www.youtube.com/watch?v=KJS7RQGONt8, accessed on 5 January 2023.

[15] Li, Haijia, Cailin Yang. Digital Transformation of Manufacturing Enterprises, *Procedia Computer Science*, vol. 187, p. 24-29, doi: https://doi.org/10.1016/j.procs.2021.04.029, 2021.

[16] Nižetić, Sandro, Petar Šolić, Diego López-de-Ipiña González-de-Artaza, Luigi Patrono, Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future, ***Journal of Cleaner Production***, vol. 274, doi: https://doi.org/10.1016/j.jclepro.2020.122877, 2020.

[17] Nugroho, Inaz Indra, Reza Pratiwi, Salsabila Rahma Az Zahro, Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia, ***IPMHI Law Journal***, vol. 1, no. 2, p. 115-129, doi: https://doi.org/10.15294/ipmhi.v1i2.53270, 2021.

[18] Prasetya, Teguh. (2020). "InfoKomputer TechGathering: Inilah Tren Pemanfaatan IoT di Industri Manufaktur." Retrieved from https://www.youtube.com/watch?v=dV_-pZ-gQRw, accessed on 5 January 2023.

[19] Reksoprodjo, Yono. Ilusi Membangun Kemandirian Industri Alpalhankam Nasional. Bekasi: CVI Publishing. 2022.

[20] Shen, W, Norrie, D.H. Agent-Based Systems for Intelligent Manufacturing: A State-of-the-Art Survey, ***Knowledge and Information Systems, an International Journal***, 1999, vol. 1, No. 2, p. 129-156, doi: https://doi.org/10.1007/BF03325096.

[21] Sreekumar, Arjun. (2020). How COVID-19 Will Impact the Defence Industry: Defence Companies Are Among The Many Industries That Must Brace For A Coronavirus Shock. Retrieved from https://thediplomat.com/2020/03/how-covid-19-will-impact-the-defence-industry/, accessed on 5 January 2023.

[22] Suryanto Janu R. (2019). Kementerian Komunikasi dan Informatika: Industri 4.0 Buka Peluang RI Jadi Ekosistem Bisnis IoT Senilai Rp 444 Triliun. Retrieved from https://www.kominfo.go.id/content/detail/18517/industri-40-buka-peluang-ri-jadi-ekosistem-bisnis-iot-senilai-rp-444-triliun/0/berita, accessed on 5 January 2023.

[23] Thales.(2023).Building Trust In IoT Devices With Powerful Iot Security Solutions, Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security#:~:text=Telit%2DCinterion%20website.,What%20is%20IoT%20security%3F,confidentiality%20of%20your%20IoT%20solution, accessed on 6 January 2023.

[24] Zhong, Ray Y., Xun Xu, Eberhard Klotz, Stephen T. Newman, Intelligent Manufacturing in the Context of Industry 4.0: A Review, *Engineering*, 2017, vol. 3, no. 5, p. 616-630, doi: https://doi.org/10.1016/J.ENG.2017.05.015.