iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VII **Month of publication:** July 2023

DOI: https://doi.org/10.22214/ijraset.2023.54840

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

Enhancing Air and Missile Defense System with IoT Solution: A Conceptual Approach

Priya Chaurasiya[1], Saara Sawardekar[2], Ruchi Rautela[3]
Vivekananda Education Society Institute Of Technology

Abstract: ***The Internet of Things (IoT) concept, technology, and military applications are presented in this paper. The authors argue that when implemented as a system solution, IoT may increase the capability of the entire system after providing a brief review of cases of partial deployment of the technology in air and missile defense (AMD) systems. The air and missile defense system has been analytically divided into four subsystems, and using a conceptual approach, each of them has been examined in terms of how it might be strengthened by the adoption of IoT solutions and how those latter might translate into the improvement of the entire AMD system. The paper divides the air and missile defense system into four subsystems and analyzes each of them conceptually to ascertain how IoT solutions can strengthen them and how this can translate into improving the entire AMD system. The IoT can streamline procedures in a variety of industries, resulting in better IoT device performance.***
Keywords: Internet of Things (IoT), Military, Air and missile defence (AMD) systems, Sensors, air safety, Data

I. INTRODUCTION

The Fourth Industrial Revolution (also known as Industry 4.0), which is characterized by the integration of the physical world of systems and machinery with the virtual one of the Internet through the exchange and real-time analysis of data using sensors embedded in equipment, has been created by dynamic technological development. Informally coined by Microsoft's CEO Bill Gates in 1995 as a concept illustrating the "thing to thing" connection, the Internet of Things (IoT) is a technology specific to the Fourth Industrial Revolution. The International Telecommunication Union was established in 1999 by EPCglobal, formally introducing the idea of IoT, by bringing together more than 100 businesses. The "ITU Internet Reports 2005: The Internet of Things" gave rise to the concept for its development. In 2014, when wireless communication technologies were just starting to take off, it started to gain popularity.

The Internet of Things (IoT) is a tool that enables the acquisition, processing, and presentation of data from various sources, including sensors.

The operation of IoT is based on three main factors:

1) Hardware, which includes sensors, actuators, and embedded communication hardware; middleware, which offers computing power and storage on demand for data analytics.
2) Presentation provides cutting-edge visualization and interpretation tools that are accessible on various platforms and created for a variety of applications. IoT is revolutionizing the private sector's approach to the creation, distribution, and management of infrastructure. Therefore, it is not surprising that more and more research is being done on IoT applications for the military, including the Internet of Battlefield Things and the Internet of Military Things more generally. The Internet of Things (IoT) has become one of the most important trends in the digital transformation of numerous industries.

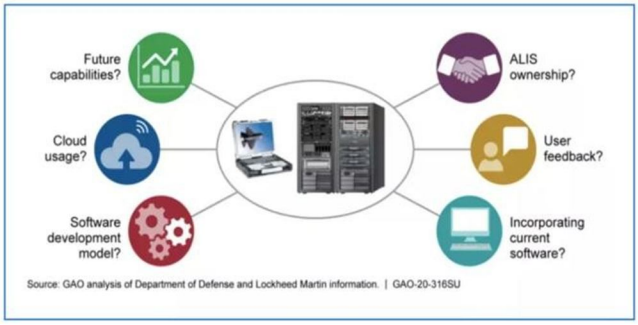
The military can gain a lot from utilizing IoT technology, both during routine operations of a military unit in times of peace and when conducting military operations. A review of the literature revealed that there aren't many studies examining the viability of using that technology by specific specialties, despite the growing interest in the potential use of IoT by the military. The most typical strategy is to treat the problem in overly general terms. Advanced weapon system design, development, and manufacturing call for specialized labs, testing, and production facilities, as well as expertise and experience that cannot be easily acquired from other industries. IoT technology has the potential to transform military operations by enhancing situational awareness and giving soldiers more information. The military uses sensors to collect data from a variety of platforms, including aircraft, weapon systems, ground vehicles, and soldiers in the field. IoT has advantages that appeal to the military, but they also make the network susceptible to cyberattacks that could jeopardize military security.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

II. INTERNET OF THINGS IN MILITARY APPLICATIONS –CURRENTSOLUTIONS

Modern technology is used in the military to create more effective systems that can adapt to the demands of a complicated battlefield. IoT is a technology for the future battlefield, and the operational military subsystems already use some of its specific solutions. Management and support for air and missile defense (AMD) are two areas where IoT is being used. For instance, the F-35 aircraft's Autonomic Logistics Information System (ALIS) makes use of IoT. ALIS combines a wide range of functionalities, including supply chain, operations, maintenance, prognostics, training, and technical data. It also integrates customer support services. With the help of web-enabled applications on a distributed network, users can access the most recent information on any of these topics from a single, secure information environment. Sensors are used by the military to collect data from a variety of platforms, such as aircraft, weaponry, ground vehicles, and deployed troops. IoT technology has the potential to completely transform military operations by giving soldiers more information and situational awareness, boosting productivity, and improving safety andsecurity.

The Autonomic Logistics Information System (ALIS) is made to keep track of the condition of the F-35 fleet and take appropriate action, like planning maintenance or ordering replacement parts, to make it better. By informing them of which aircraft are prepared for take-off, it also assists military leadership in maintaining control of the fleet. ALIS's software is designed to assist with mission planning and information recording for debriefing. Additionally, a tool in ALIS keeps track of pilot and maintenance training, keeping them up to date on any advancements in the F-35's technology or capabilities. ALIS is a crucial component of the F-35 program that enables the fleet's daily operations, including mission planning, flight operations, maintenance, and logistics. To guarantee that the F-35 fleet is always prepared for action, the system is made to be dependable and functional in a range of environmental conditions. Overall, ALIS is a thorough system that gives the ability to watch over and maintain the F-35 fleet, ensuring that it is constantly prepared to meet mission requirements.



Even though the F-35 plane has been worked on and tested for a long time, the computer program that runs it, called ALIS, is still not working properly. This is a big problem because ALIS is very connected to the F-35. The ALIS program often has wrong or missing information, so the people who take care of the F-35 have to do extra work to keep track of things that should have been done automatically by ALIS. This process is both time-consuming and risky, as there is a chance that critical data could be overlooked when tracking information using Excel spreadsheets. The F-35 program has been plagued with unforeseen increases in development, production, and maintenance and sustainment activities. The ALIS system also has several unresolved cybersecurity vulnerabilities, partially because Lockheed Martinstarted shipping F-35s before ALIS was complete. The program office now plans to make gradual improvements to ALIS and eventually rename it, including smaller hardware and improved program data access. The program has yet to identify a new systemto replace ALIS.

The F-35 personnel who use ALIS have reported that the user experience is poor, and the interface is not intuitive, making it hard to navigate. Standard functions can take much longer to complete than expected, and the training application is not being used in anyof the five locations visited. The application is not user-friendly, andthey prefer to use legacy systems instead. The hardware required to transport ALIS is bulky and heavy, with each server unit weighing approximately 200 pounds and requiring at least two people to lift. Several server units need to be taken on deployment, and they require a whole room to operate, making it challenging to find a place to store them on a ship. Lockheed is making progress on a smaller, more portable version of ALIS, which is expected to be released after ALIS 2.0. The new version will be easier to transport and operate, and Lockheed is on track to certify and test the portable version of ALIS in the first quarter of 2015. The ALIS system is continually being improved and updated to take into account user feedback and improve the user experience.

The Department of Defense has acknowledged that the current system, ALIS, needs to be redesigned and replaced with a new system called the F-35 Operational Data Integrated Network (ODIN). However, there are still some critical questions that need to be answered about the effort. For example, it is unclear how much of ALIS will be incorporated into ODIN, and whether the Department has access to the data it needs to play a more active role in managing the new system. The figure below illustrates the technical and programmatic uncertainties that remain. The F-35 Joint Program Office has completed the initial deployment of ODIN hardware, which replaces all first-generation unclassified ALIS servers in the field. Lockheed Martin is currently in negotiations with the Department of Defense to compensate for the new government-owned system, ODIN. The new software, called ALIS, enables daily operations of the F-35 fleet, ranging from mission planning and flight scheduling to repairs and scheduled maintenance, as well as the tracking and ordering of parts.

The Department of Defense (DOD) must carefully consider and assess several questions as it proceeds with developing its new system. Additionally, the DOD has not yet developed a performance measurement process for the Autonomic Logistics Information System (ALIS) or determined how ALIS issues affect the readiness of the F-35 fleet. Therefore, it is crucial for the DOD to incorporate these efforts into its current and future systems. ALIS is a critical system that enables daily operations of the F-35 fleet, including mission planning, flight scheduling, repairs, and maintenance. The new version of ALIS, ALIS 2.0, will provide more advanced reporting features to manage the fleets and analyze data from the aircraft. The missile launcher is another critical subsystem of air and missile defense systems that is responsible for firing the missile to intercept the incoming threat. The missile launcher must be able to fire a wide range of missiles and provide accurate targeting data to ensure that it intercepts the incoming threat. Overall, the DOD must carefully consider and assess several questions as it proceeds with developing its new system, and it must incorporate efforts to develop a performance measurement process for ALIS and determine how ALIS issues affect the readiness of the F-35 fleet into its current and future systems.

A. IBCS

The Integrated Air and Missile Defence Battle Command System (IBCS) is a cutting-edge command-and-control (C2) system that has been specifically designed to provide a comprehensive and clear understanding of the entire battlespace. By incorporating both existing and upcoming sensors and weapon systems, IBCS facilitates seamless integration and interoperability with joint C2 operations as well as the ballistic missile defence system. With the implementation of this system, the commander gains access to a complete and detailed overview of the air situation, thereby enhancing their decision-making capabilities and overall effectiveness in military operations.

Integrated Battle Command System (IBCS)

The Internet of Things (IoT) can be used effectively, and the IBCS is a prime example of this. It highlights the vast opportunities that can be created when IoT is incorporated into air and missile defiance systems. The military is able to gather important information by mounting sensors on a variety of platforms, including aircraft, weaponry, ground vehicles, and soldiers in the field. By continuously tracking, enhancing, and efficiently allocating various resources and processes, including fire-control systems, the military can revolutionize how equipment is maintained and managed. The IoT also has the potential to significantly enhance situational awareness on the battlefield, from a global perspective all the way down to individual soldiers, empowering commanders at every level from company to platoon to squad.

Northrop Grumman recently made an exciting announcement regarding its Integrated Battle Command System (IBCS). The system has successfully completed its Initial Operational Test and Evaluation (IOT&E), marking a crucial milestone before the US Army can move forward with the program and transition it into Full-Rate Production. The IBCS demonstrated its capabilities during flight tests at the White Sands Missile Range (WSMR), where it effectively detected, tracked, and intercepted various threats, including a high-speed, high-performance tactical ballistic missile and two cruise missile surrogates during an electronic attack. This impressive performance has been commended by Christine Harbison, Vice President and General Manager of Combat Systems and Mission Readiness at Northrop Grumman. Harbison expressed that throughout the IOT&E process, IBCS has exhibited its ability to empower war fighters by providing them with more accurate information and enabling faster decision-making. She emphasized that IBCS is not only prepared to tackle present-day threats but also equipped to handle future challenges, thereby solidifying the realization of Joint All-Domain Command and Control (JADC2). With the successful conclusion of IOT&E, the path has been cleared for the US Army to proceed with the full-rate production of IBCS, a cutting-edge system specifically designed for their needs.

III. EXAMPLE IMPLEMENTATION OF THE IOT CONCEPT IN AIR DEFENCE ARTILLERY SYSTEMS

The potential of IoT in air defence extends beyond the aforementioned examples. In order to further illustrate the potential applications of IoT in air defence, this section will delve into the concept of integrating IoT into existing air defence artillery weapon systems. Counter rocket, artillery, and mortar (C-RAM), which refers to a collection of systems utilized for detecting and neutralizing incoming rockets, artillery, and mortar rounds in mid- air before they reach their intended targets on the ground, or alternatively, for providing early warning signals.

Counter Rocket, Artillery, and Mortar (C-RAM) is a system designed to detect, track, and intercept incoming rockets, artillery, and mortar rounds. The implementation of the Internet of Things (IoT) in C-RAM can provide a more efficient and effective way of detecting and intercepting these threats.One way IoT can be implemented in C-RAM is through the use of sensors. These sensors can be placed in strategic locations to detect incoming threats. The sensors can then send data to a central system, which can analyze the data and determine the best course of action. This can include activating countermeasures such as jamming or intercepting the incoming threat.

Another way IoT can be implemented in C-RAM is through the use of drones. Drones equipped with sensors and cameras can be used to detect incoming threats and provide real-time data to the central system. The drones can also be used to intercept the incoming threat, providing a more efficient and effective way of neutralizing the threat.

2010 TEST FIRE OF A CRAM,BALAD,IRAQ

IoT can also be used to improve the maintenance and upkeep of C-RAM systems. Sensors can be placed on the C-RAM systems to monitor their performance and detect any issues. This can help prevent downtime and ensure that the systems are always ready to detect and intercept incoming threats.

In conclusion, the implementation of IoT in C-RAM can provide a more efficient and effective way of detecting, tracking, and intercepting incoming threats. By using sensors, drones, and other IoT devices, C-RAM systems can be more responsive and better equipped to handle the challenges of modern warfare.

IV. A SYSTEM APPROACH TO THE IOT IN AIR AND MISSILE DEFENSE

The concept of the system approach was initially introduced by Ludwig von Bertalanffy, the founder of general system theory, and Norbert Wiener, the creator of cybernetics. In its current application, the system approach views objects under examination as a collection of interconnected elements forming a cohesive whole within a specific context. This approach has gained significance due to the increasing need for continuous improvement and enhancement of air and missile defense systems. This requirement arises from the ever-evolving nature of threats, which are expected to take on new forms in the future. Ludwig von Bertalanffy's general system theory aimed to provide a comprehensive explanation of systems across all scientific disciplines. Consequently, this concept has garnered considerable attention in his work and has found widespread application in various scientific fields. The US Department of Defence acknowledges the increasing threat of missile attacks from rogue states and powers that seek to challenge the US, its allies, and partners. These threats include ballistic and cruise missiles, as well as hypersonic vehicles. To effectively counter this growing danger, it is crucial to continuously update and enhance defence capabilities through technological advancements. This is especially true in the realm of air and missile attack and defence systems, where there is an evident lack of technological balance between the two sides. Developing and maintaining defence systems requires highly advanced technologies and substantial investments. In this context, the Internet of Things (IoT) emerges as a transformative technology that has the potential to fortify the entire Air and Missile Defence (AMD) system, rather than just improving certain components. By leveraging IoT technology, military operations can undergo a revolution, empowering soldiers with greater access to information and situational awareness, facilitating communication, and optimizing logistics. The military has already adopted IoT-enabled devices such as wearables, sensors, and beacons, which enable the tracking of soldiers and equipment, monitoring of their health and performance, and provision of real-time data on the battlefield. Moreover, these devices can also be utilized to monitor and analyse the surrounding environment, track enemy movements, and enable the development of IoT applications for military purposes.

Air and missile defence has two types of environments: the closer and the further environment.

1) The further environment includes the economic, technological, international, political and legal, and socio- demographic areas that determine the financial and tactical capabilities of the AMD provider, the state of AMD, the employment of military units, and the support of the system by human resources.
2) The closer environment includes own aircraft, protect objects, external sources of information, and air threat, which are tactical assets that have an influence on the battlefield and should be considered in the IoT system of the AMD.
3) The further environment describes the strategic situation of the AMD system of the state.
4) The IoT technology can strengthen the whole AMD system, not just some of its components, and revolutionize military operations, providing soldiers with more information and situational awareness, enhancing communication, and streamlining logistics.
5) The US Department of Defence recognizes the growing missile threats posed by rogue states and revisionist powers to the US, its allies, and partners, including ballistic and cruise missiles, and hypersonic vehicles.
6) The military needs to constantly update their defence capabilities technologically to counter the growing threat.

Air and missile defense systems consist of several subsystems that work together to provide a comprehensive defense system. The subsystems of air and missile defense systems include the power plant, radar set, engagement control station, communication equipment, and missile launcher. The power plant provides the necessary power to operate the system, while the radar set detects incoming threats and provides real-time data to the engagement control station. The engagement control station processes the data from the radar set and provides targeting information to the missile launcher. The communication equipment enables communication between the subsystems and with other defense systems. The missile launcher launches the missile to intercept the incoming threat. Additionally, air defense systems may include interceptors or fighter aircraft that take off from airbases to intercept incoming threats. Overall, the subsystems of air and missile defense systems work together to provide a comprehensive defense system that can detect and destroy incoming threats.

A. *Air and Missile defense Consists of five Basic Subsystems*

1) Power plant,
2) Radar set,
3) Engagement control station,
4) Communication equipment, (5)The missile launcher.

a) *Power Plant: The* power plant is a critical subsystem of air and missile defense systems. It provides the necessary power to operate the system, including the radar set, engagement control station, and launcher. The power plant can be a generator or a battery, depending on the system's requirements. The generator can be powered by diesel, gas, or other fuels, while the battery can be rechargeable or non-rechargeable. The power plant must be reliable and able to operate in harsh environments, including extreme temperatures and weather conditions. It must also be able to operate for extended periods without maintenance or refueling. The power plant's capacity must be sufficient to meet the system's power requirements, including peak power demands during missile launches. The power plant's design must also consider the system's mobility requirements, as air and missile defense systems are often deployed in remote or austere locations. Overall, the power plant is a critical subsystem of air and missile defense systems, providing the necessary power to operate the system and ensuring its reliability and effectiveness in defending against incoming threats.

b) *Radar Set*: The radar set is a critical subsystem of air and missile defense systems. It detects incoming threats and provides data to the engagement control station, which processes the data and determines the best course of action to engage the incoming threat. The radar set can be either a ground-based or a sea-based system, depending on the specific system. The radar set must be able to detect a wide range of targets, including ballistic missiles, cruise missiles, and aircraft, and must be able to operate in a variety of environmental conditions, including extreme temperatures and high altitudes. The radar set must also be able to provide accurate data on the location, speed, and trajectory of the incoming threat to enable effective targeting by the engagement control station. The radar set is typically located near the launcher to minimize data transmission losses and ensure that the engagement control station has sufficient data to operate.

The radar set is also responsible for providing data to the air defense command, control, and intelligence system, which provides situational awareness and targeting data on threat aircraft, cruise missiles, and unmanned aerial systems. Overall, the radar set is a critical subsystem of air and missile defense systems, providing the necessary data to detect and engage incoming threats and ensuring that the system is reliable and able to operate in a variety of environmental conditions.

c) *Engagement Control Station*: The engagement control station is a critical subsystem of air and missile defense systems. It processes the data from the radar set and determines the best course of action to engage the incoming threat. The engagement control station can be either a ground-based or a sea-based system, depending on the specific system. The engagement control station must be able to process a wide range of data, including the location, speed, and trajectory of the incoming threat, and must be able to make rapid decisions on the best course of action to engage the threat. The engagement control station is typically located near the launcher to minimize data transmission losses and ensure that the launcher has sufficient data to operate. The engagement control station is also responsible for providing data to the air defense command, control, and intelligence system, which provides situational awareness and targeting data on threat aircraft, cruise missiles, and unmanned aerial systems. The engagement control station is also responsible for coordinating with other air and missile defense systems to provide a more comprehensive and effective defense system. Overall, the engagement control station is a critical subsystem of air and missile defense systems, providing the necessary data to engage incoming threats and ensuring that the system is reliable and able to operate in a variety of environmental conditions.

d) *Communication Equipment*: Communication equipment is a critical subsystem of air and missile defense systems. It provides the necessary communication links between the various subsystems of the system, including the radar set, engagement control station, launcher, and air defense command, control, and intelligence system. The communication equipment can be either a wired or wireless system, depending on the specific system. The communication equipment must be reliable and able to operate in a variety of environmental conditions, including extreme temperatures and high altitudes. It must also be able to provide secure communication links to prevent interception by the enemy. The communication equipment is typically located near the engagement control station to ensure that the system has sufficient communication links to operate. The communication equipment is also responsible for providing data to other air and missile defense systems to provide a more comprehensive and effective defense system. Overall, the communication equipment is a critical subsystem of air and missile defense systems, providing the necessary communication links to ensure that the system is reliable and able to operate in a variety of environmental conditions.

e) *The Missile Launcher*: The missile launcher is a critical subsystem of air and missile defense systems. It is responsible for firing the missile to intercept the incoming threat. The missile launcher can be either a ground-based or a sea-based system, depending on the specific system. The missile launcher must be able to fire a wide range of missiles, including surface-to-air missiles and anti-ballistic missiles, and must be able to operate in a variety of environmental conditions, including extreme temperatures and high altitudes. The missile launcher must also be able to provide accurate targeting data to the missile to ensure that it intercepts the incoming threat. The missile launcher is typically located near the engagement control station to ensure that the system has sufficient targeting data to operate. The missile launcher is also responsible for providing data to the air defense command, control, and intelligence system, which provides situational awareness and targeting data on threat aircraft, cruise missiles, and unmanned aerial systems. Overall, the missile launcher is a critical subsystem of air and missile defense systems, providing the necessary capability to intercept incoming threats and ensuring that the system is reliable and able to operate in a variety of environmental conditions.

V. CONCLUSIONS

In combat, it is important to make decisions quickly. This is because technology is changing and getting better, especially in air combat. There are new weapons that can fly fast and are hard to detect. These weapons can be controlled by computers, and in the future, computers might be able to control the whole combat process. The internet of things (IoT) is a technology that can help with this. It is already being used in some parts of the military. One way it could be used is to help with the logistics of a battle. For example, it could help with moving supplies and equipment. Hypersonic weapons are another type of weapon that can fly really fast. The United States is working on developing these weapons for the Army, Navy, and Air Force.

Using IoT as a system solution for AMD systems would make them stronger and better. This is really important, especially when there are lots of threats to air and missile defence systems. But it's also important to know that using IoT can bring new dangers too. It can make battle systems more likely to be attacked by hackers. Since the 1990s, the internet has become a big part of how conflicts happen. Using IoT can help make military decisions, support logistics, and control firing, which is really important for air and missile defence. IoT sensor networks help collect important information from the outside world and from inside the system and use that information to make good decisions. IoT is used in lots of different ways, like controlling traffic, measuring things like electricity use, watching the environment, and managing resources.

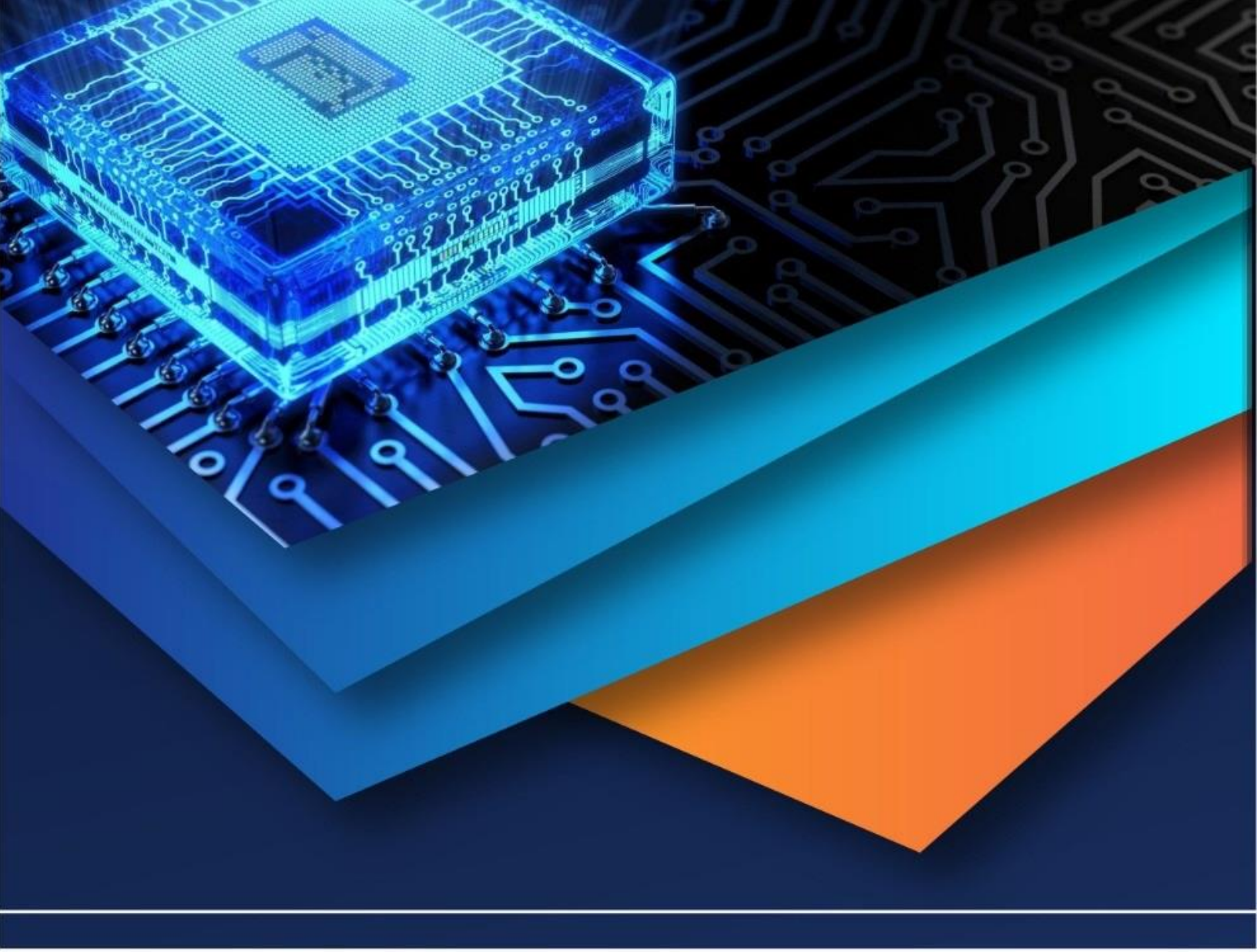
IoT can take the place of the command centre and either support the commander's decision-making process or even fully automate it. John K. HAWLIE AND ANNA L. Mares argues that while automation and other cutting-edge technologies lessen the immediate need for people, they simultaneously increase their importance to the overall effectiveness of the system. On a variety of platforms, including aircraft, weapon systems, ground vehicles, and even soldiers in the field, the military collects data using sensors. The military is moving toward an integrated warfare strategy, using secure communication networks like the Command, Control, Battle Management, and Communications System (C2BMC) of the Missile Defence Agency, which is an example of an IoT-enabled warfighting network. With built-in device connectivity and management features, the IoT device management platform makes management simpler.

VI. ACKNOWLEDGMENT

Scientific research was carried out in the framework of the project "Automation of information and decision-making processes in air defence under the conditions of modelled air threat of troops and critical infrastructure facilities"

REFERENCES

[1] https://www.lockheedmartin.com/en- us/news/features/2017/internet-of-things-transofrming- modern-warfare.html
[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7368922/
[3] https://irp.fas.org/doddir/army/atp3-01-16.pdf
[4] https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution
[5] https://www.forbes.com/sites/bernardmarr/2018/09/02/wh at-is-industry-4-0-heres-a-super-easy-explanation-for- anyone/
[6] https://www.mckinsey.com/featured-insights/mckinsey- explainers/what-are-industry-4-0-the-fourth-industrial- revolution-and-4ir
[7] https://www.ibm.com/topics/industry-4-0
[8] https://www.i-scoop.eu/industry-4-0/
[9] https://www.matellio.com/blog/iot-in-military/
[10] https://asb.army.mil/Portals/105/Documents/2010s/2016%2 0A%20The%20Military%20Benefits%20and%20Risks%20of%2 0the%20Internet%20of%20Things%20Report.pdf?ver=B8FJk GnH43LJVsa0X9py9A%3D%3D
[11] https://www.academia.edu/40159897/Internet_of_Things_i n_Air_and_Missile_Defence_A_System_Solution_Concept
[12] https://idstch.com/cyber/internet-things-battlefield/
[13] https://breakingdefense.com/2022/11/armys-ibcs-wraps-up- initial-operational-testing/
[14] https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2022/budget_justification/pdfs/03_RDT_and_E/RDT E_Vol2_MDA_RDTE_PB22_Justification_Book.pdf
[15] https://idstch.com/cyber/internet-things-battlefield/
[16] https://www.armyrecognition.com/russia_russian_army_ligh t_heavy_weapons_uk/zu-23_zu-23-2_anti-aircraft_23mm_twin_gun_technical_data_sheet_specificatio ns_information_descriptio.html
[17] https://forum.allaboutcircuits.com/threads/strain-gauge- question.186248/
[18] https://www.researchgate.net/publication/273518100_On_the_history_of_Ludwig_von_Bertalanffy's_General_Systemolo gy_and_on_its_relationship_to_cybernetics_part_III_convergences_and_divergences
[19] https://www.armed- services.senate.gov/imo/media/doc/NNC_FY23%20Posture% 20Statement%2023%20March%20SASC%20FINAL.pdf
[20] https://tnsr.org/2022/09/technology-acquisition-and-arms- control-thinking-through-the-hypersonic-weapons-debate/
[21] https://www.airandspaceforces.com/article/the-evolution- of-space-based-isr/
[22] https://www.softwareag.com/en_corporate/resources/iot/g uide/internet-of-things.html
[23] https://www.mdpi.com/1424-8220/20/21/6076
[24] https://www.techtarget.com/iotagenda/definition/Internet- of-Things-IoT
[25] https://www.nato.int/cps/en/natohq/topics_61741.htm
[26] https://www.marines.mil/Portals/1/Publications/MCWP%20 3-21.2%20Aviation%20Logistics.pdf
[27] https://www.cbo.gov/publication/58924
[28] https://www.mdpi.com/1424-8220/20/21/6076
[29] https://apps.dtic.mil/sti/pdfs/ADA557876.pdf
[30] https://secwww.jhuapl.edu/techdigest/Content/techdigest/p df/V22-N03/22-03-Krill.pdf
[31] https://news.northropgrumman.com/news/releases/northro p-grummans-ibcs-ready-for-fielding-connecting-the- battlespace
[32] https://breakingdefense.com/2022/11/armys-ibcs-wraps-up- initial-operational-testing/
[33] https://www.govinfo.gov/content/pkg/CRPT- 117srpt130/html/CRPT-117srpt130.htm



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY