International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 09 Sep. 2024, pp: 52-58 www.ijaem.net ISSN: 2395-5252

Applying Cyber Security Engineering to Aerospace Engineering Sector

Felix Ale[1], Abdullahi Ayegba[2], Desmond Wysenyuy[3], Iruemi Olohimai Juliet[4], Abegunde Linda Olukemi[5], Mba Tochukwu William[6], NdahiAisha[7], and Enyum Eno U[8]

[1,2,4,8]*Department of Engineering and Space Systems, National Space Research and Development Agency, Abuja, Nigeria,*
[5]*Cooperative Information Network, National Space Research and Development Agency, Osun State, Nigeria,*[6]*United Nations, African Regional Centre for Space Science and Technology Education in English, O.A.U, Ile-Ife, Nigeria,*
[6]*Management and Research Analysis, School of Space and Earth Observation, Arizona State University, USA,*
[7]*Interplanetary Initiative, Arizona State University, USA,*

Date of Submission: 01-09-2024 Date of Acceptance: 10-09-2024

ABSTRACT
The aim of this research work was to study how cyber security Engineering can be applied to Aerospace Engineering sector. The study employed review and explanatory research methods, drawing from a variety of online research works and library materials. The results show that cyber security Engineering plays critical roles in aerospace or space science and technology, such as securing communication systems, securing of Data Storage application, ground station security, launch vehicle security, vulnerability management, aerospace supply chain security, etc. From the results, it was concluded that cyber security engineering is very paramount when integrated with the aerospace sector, as it will help to achieve or maintain a secured space segment, ground segment, and the communication link between the space and the ground segments, including interlinking with other space or ground segments or others in the supply chain. It was recommended that some various cyber security models or methods for securing each of these segments be investigated and discussed in detail in future work.

Keywords: Aerospace, Cyber security, Data storage, Engineering, Space Technology

I. INTRODUCTION

Aerospace Engineering deals with the design, construction, and study of the science behind the forces and physical properties of aircraft, rockets, flying craft, and spacecraft. In a simple way, aerospace engineering deals with the design of aircraft and spacecraft. The field also covers their aerodynamic characteristics and behaviors, airfoil, control surfaces, lift, drag, and other properties. Aerospace engineering is divided into two major and overlapping branches, which are aeronautical engineering and astronautical engineering. Aeronautics deals with aircraft that operate in Earth's atmosphere, and astronautics deals with spacecraft that operate outside the Earth's atmosphere (Encyclopedia.com).

Recently, cyber-physical systems have become an emerging paradigm for the control and management of the ever-growing number of cyber-connected devices and have experienced an increased use in different applications as a result of their benefits, such as their ability to seamlessly integrate systems from the cyber and physical domains to create value (Saqib et al., 2018). Also, across various parts of the world, aerospace is taking off, and the industry is on the verge of unprecedented growth, accompanied by ongoing digital transformation. But this growth and the complexity of digitization are associated with greater information security risk, which can result in both effective cybercrime and serious safety and security breaches (BSI, 2020). Ordinarily, it can be said that every system is prone to risks, be it aerospace engineering, manufacturing systems, information technology, oil and gas, logistics or supply chain, etc., which are some examples of the domains where risks are seen in day-to-day aspects of their operation (Vinyas, 2023). The application of encryption or converting of information to code can be seen in numerous domains, including medical science, military, as well as geographic satellite images. Confidentiality, authenticity, security, privacy, and integrity of data have become vital issues for communication and storage of images, especially when dealing with the internet, a channel that is insecure (Al-Khasawnehet al., 2020). The aviation industry makes use of radio frequency to communicate between the aircraft and the Airport Communication Centre, the same way space science and technology organizations make use of communication or electromagnetic waves to communicate between the satellite or spacecraft and ground station or other satellite through a crosslink. This communication link between the ground segment or facility on the earth and the space segment, such as the satellite or aircraft, needs adequate security to avoid communication signal breaches, leaks, or corruption. The importance of aerospace engineering in Nigeria in particular and the world in general cannot be over emphasized. Being the field that covers both aviation and space science and technology, aerospace engineering has the potential to boost the economy of Nigeria through various industries, and as well create employment opportunities for many people in the fields of agriculture, oil sector, mining, environment, communication, environmental management, space exploration, education, etc. As a result of the various key roles played by aerospace engineering or the aerospace sector in the general economy, and with the continuous increase in cyber threats and attacks in society, according to some studies, there is a need to study how cyber security can be applied to aerospace engineering in order to ensure integrity, confidentiality, and availability in the operation, hence, the reason for this research work.

II. METHODOLOGY

In this research work, the materials used were secondary materials, which are mostly published research works in the field and other related fields. Other secondary data used were library materials and YouTube videos. The research adopted review and explanatory research methods to discuss the research question.

III. RESULT AND DISCUSSION

Applying Cyber Security Engineering to Aerospace Engineering

How is cyber security engineering applicable to aerospace engineering or the aerospace sector? The following are some areas where cyber security engineering can be applied to aerospace engineering or the aerospace sector.

3.1. Cybersecurity Engineering ensures secure communication systems: Spacecraft or satellite communication is defined as the use of satellites to provide communication links between spacecraft and earth stations or various points on the earth. This is the same in the case of aircraft in the air and the airport terminals or Airport Communication Center. The design of secure communication systems for aircraft and spacecraft operations is very important as it will help to achieve the integrity, confidentiality, and authenticity of data transmitted between spacecraft, or satellites in space and ground stations, or the aircraft and the ground communication center or airport communication center. A secure communication system is necessary in the transmission or sending of data from the server to the users. This is done through encryption, which deals with the use of algorithms and protocols to protect data from unauthorized access; Secure Communication Protocols which involve the use of secure communication protocols such as SSL, IPsec, and SSH to prevent data in transit from unauthorized access. Secure communication Systems for satellite or spacecraft data can also be done through the information authentication method, which involves the verification of the identity of communicating parties in order to prevent intrusion, impersonation, and illegal or authorized access. Communication security helps in defending and protecting information from unauthoirsed interception, use, or modification of communications networks in a global sense, from voice to images to data (Sergio and Luciana, 2016). According to Lucas (2024), to ensure secure communication between the satellite constellation and the ground segment, there was a need for two layers of authentication methods. It was reported in the same works that when implementing secure communication protocols, encryption algorithms, or multi-step authentication processes, even though these systems may require repeated data exchanges or large payloads that strain the available bandwidth, security systems must be built in a way so that they can operate under these constraints, where the balance between security and efficient bandwidth is important.

3.2. Cybersecurity secures data storage applications: Data storage security deals with the protection of storage resources and the data stored on them from intentional or accidental damage, as well as unauthorized users and access (Ale et al., 2024). Secure Data Storage is defined as computing processes and technologies used to ensure stored data security and integrity, including physical protection of the hardware on which the data is stored as well as security software. Information in the aerospace sector is very important, with some even classified or restricted; hence, secure data storage is necessary to ensure data safety. Some ways of carrying out this are regulating the accessibility to each data storage device/software, protection of data storage devices and data itself against viruses, worms, and other data corruption threats, adoption, as well as implementation of layered storage security architecture and storage device and infrastructure security.

3.3. Cybersecurity Engineering helps in Ground Station Security: A satellite ground station, or Earth station is defined as a location on the earth's surface with a large antenna, computer and other technical equipment that enables the facility to receive signals or data from the satellite in space. A satellite ground station is defined as the station or facility built for the collection and streaming of remote sensing satellite data to a variety of users and applications(https://www.essearth.com>satellite).The ground station provides the physical-layer infrastructure to communicate with the space segment. Where the spacecraft is a vehicle not in geostationary orbit, the mission may require numerous ground stations across the planet to maintain communications with the space segment throughout its orbit (Evan et al., 2021). The communication link between these several ground stations for this satellite needs proper security, and it is provided by cyber security. A ground station can also be described as the combination of some computers and antennas to send and/or receive electromagnetic waves to and from a satellite in space. Although, the traditional ground segment has physical infrastructure that has traditionally operated on private networks, providing an air gap that protects from attack (Evan et al., 2021), it can also be affected by cyberattack. Ground station security deals with the design and implementation of security architecture that will protect ground stations and control centers that communicate with satellites or aircraft. The protection of ground stations using cyber security involves physical security, which involves protecting ground stations and control centers from unauthorized access and physical tampering; secure software development, which involves developing software for ground station systems using secure coding practices and vulnerability management; and well as Network Security which involves the protection of ground station networks from cyber threats or attacks.Ground stations are responsible for communicating with satellites, tracking their trajectory, and receiving and processing data.

Plate1: Photo of National Space Research and Development Agency (NASRDA)ground station, Abuja, Nigeria

3.4. Cyber security engineering is applicable to launch vehicle security: A launch vehicle is defined as a rocket-powered vehicle used for transporting spacecraft or satellites from the earth to orbit or space. This vehicle operates based on programmes or information sent to or stored in it during its journey in space. It is a command that is generally called telemetry, tracking, and command. They allow data or information to be sent and received between the ground and the satellite or spacecraft in the orbit. This signal or information is sent between the spacecraft and the earth through a communication link. This communication link can be compromised or attacked if not properly secured using cybersecurity. In fact, the message or signal sent from the ground station can be diverted or corrupted through a cyberattack. Even a strange message or command can be sent by attackers to it, and the satellite will start to misbehave or perform abnormally. In the satellite RF domain, it was found out that the physical distance and visibility of space systems raises novel problems for broadcast and interactive communications, and attackers have exploited these dynamics to compromise sensitive data, transmit illicit broadcasts, and deceive satellite customers. The cyber security engineers can contribute to mitigating these issues by considering the unique hardware and physical constraints impacting cryptography and verification in satellite communications (James and Ivan, 2022) and, by extension, aerospace in general, which is a cybersecurity measure. The securing of launch vehicles with cybersecurity can be done through the implementation of secure communication protocols to protect data transmitted between launch vehicles and ground stations, carrying out regular security audits, as well as proper access control and authentication mechanisms. There is also a need for the updating of software and systems with the latest security trends regularly.

3.5. Cyber security engineering helps in data encryption: Data encryption is defined as the method of converting information into code using an algorithm. The encrypted information or data is called encoded data. It can only be accessed by the receiver who has the mechanism for converting it from codes to the original information. The process is called decryption. Encryption of data helps achieve data confidentiality, integrity, and authenticity. This is very important: aerospace or space science and technology. Security and confidentiality of data are important as well because security violations can impact the privacy and reputation of users. Thus, each data type is equipped with its own means of protection from illegal or unauthorized access, such as data encryption (Al-Khasawneh et al., 2018). This is necessary as there has been a rapid increase in the volume and level of electronic data exchange today (Al-Khasawneh et al., 2020). The information to be sent between the ground, which is downlink and uplink, or between satellites or aircraft, which is crosslink, must be encrypted because when it is attacked or manipulated by another person, it will cause a problem. In addition to an attack, it will make the information accessible to people, including classified information that is to be restricted. In other words, encryption of data shared between space agencies, organizations, or international bodies is very paramount.Satellite or spacecraft data encryption can be achieved through some methods, such as symmetric encryption, which involves the use of the same key for encryption and decryption; asymmetric encryption, which involves the use of a public key for encryption and a private key for decryption; and hashing, which involves creating a digital fingerprint for data integrity verification (“What is encryption?, www.cloundfare.com”).

3.6. Cyber-Physical Systems Security: A cyber-physical system (CPS) is defined as the composition of independently interacting components, including communications and control systems and computational elements. Cyber-physical systems primarily transmute how we interact with the physical world, with each system requiring different levels of security based on the sensitivity of the control system and the information it carries (Charalambos et al., 2015). Cyber-physical systems can be defined as the systems that integrate computational algorithms, networking, and physical processes to interact with the physical world. Network technology has significantly improved due to the growing use of Cyber-Physical Systems (CPS) in various industries, including healthcare, transportation, and communication (Sandeep and Alankrita, 2023). Cyber-Physical Systems Security helps to protect some systems of the aerospace sector that are physical from cyber threats or attacks. Cyber-physical system security measures can be achieved through access controls and authentication, redundancy and backup systems, regular software updates, and patching.

3.7. Vulnerability Management: The term, vulnerability is defined as a process or a condition of something being prone to danger or likely to suffer an attack. Vulnerability management is defined as the continuous discovery, prioritization, and resolution of security vulnerabilities in an organization’s IT infrastructure and software (ibm.com). Vulnerabilities are weaknesses or other conditions in an organization that a cyber threat actor, such as a hacker or other attacker, can exploit to adversely affect data security (Sean, 2018). A security vulnerability is any flaw or weakness in the structure, other or implementation of a network or networked asset that hackers can exploit to launch cyber attacks, gain unauthorized access to systems or data, or otherwise harm an organization. Vulnerability management involves identifying, assessing, and mitigating vulnerabilities in space-based systems. This assessment or identification of the likelihood of risks is to be carried out on aircraft and air traffic control centers, as well as spacecraft and satellite systems, ground station and control center systems, communication networks and protocols, and software and firmware used in space missions. It involves the detection of potential vulnerabilities through regular security audits and risk assessments, evaluating the seriousness and impact of identified vulnerabilities, and adopting measures to address vulnerabilities.

Vulnerability detection can be carried out using the following methods: These are; vulnerability scanning, which deals with the scanning done to find vulnerabilities in computers, applications, or networks. A scanner (software) is used to identify vulnerabilities that arise from misconfiguration and flawed programming within a network; the second one is penetration testing, which deals with the practice of testing an IT asset for security vulnerabilities that an attacker could potentially exploit. Penetration testing can be automated or manual. It can also test security policies, employee security awareness, the ability to identify and respond to security incidents, and adherence to compliance requirements. The third method is Google hacking, which involves the use of a search engine to locate security vulnerabilities. This is achieved through advanced search operators in queries that can locate hard-to-find information or data that has been accidentally exposed due to the misconfiguration of cloud services. Mostly, these targeted queries are used to locate sensitive information that is not intended for public exposure (Muhammad et al., 2023).

3.8. Cybersecurity helps in Aerospace Supply Chain Security: Cybersecurity of the supply chain is a safety measure that focuses on the management of the required cyber security relating to information technology systems, software, and networks. Supply chain management has a high risk of being threatened by malware, cyberterrorism, and data theft. The supply chain cyber security activities are carried out to reduce the risks, including sole-purchase from trusted vendors and disconnection of critical machines from external networks (Latif et al., 2021). According to the result of the same work through their analysis, they found out that information exchange, agility, and visibility increase through digital technology. However, there are some threats and risks that arise in this supply chain. Thus, Abel and Shareeful (2019) described that cyber security within the supply chain provides organizations with secure network facilities to meet business objectives as a whole. Aerospace supply chain security refers to the protection of the supply chain from unauthorized access, tampering, and disruption. The aerospace supply chain comprises all the companies, individuals, and organizations involved in the design, development, production, and delivery of aerospace products and services.

3.9. Cyber security Engineering helps in intrusion detection: An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. There are two types of intruders, which are external intruders, who are unauthorized users of the machines they attack, and internal intruders, who have permission to access or use the system with some restrictions. The traditional prevention techniques such as user authentication, data encryption, avoiding programming errors and firewalls are used as the first line of defense for computer security. But despite these, if a password is weak and is compromised, user authentication cannot prevent unauthorized use, firewalls are vulnerable to errors in configuration and ambiguous or undefined security policies. Hence, they will be generally unable to protect against malicious mobile code, insider attacks and unsecured modems (Ajith, et al, 2014). This is why intrusion detection system provided by cyber security engineering in necessary. An Intrusion Detection System is a security tool that monitors a computer network or systems for malicious activities or policy violations (Ale et al., 2024). It is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused (Ajith et al., 2014). This is done by detecting unauthorized access, potential threats, and abnormal activities by analyzing traffic and alerting administrators to take action. It is very crucial for maintaining network security and protecting sensitive aerospace information from cyberattacks. Cybersecurity ensures that the system automatically detects and blocks the network attacks and browser attacks, protects applications from vulnerabilities, checks the contents of one or more data packages, and detects malware that is coming through legal means (Minweiet al., 2032). In other words, an intrusion detection and prevention system is another method of ensuring secure communication systems in aerospace and space science and technology, as it is a progarmme used for detecting suspicious activities and generating alerts to notify the necessary person or groups for immediate action. Data intrusion detection in aerospace engineering can be achieved through the following ways: monitoring of satellite and aircraft data transmissions, identifying unusual patterns or behaviors in the data transmissions, checking for known attack patterns or malware signatures in the data, and analysing the behavior of the data transmissions to detect potential threats, etc.

IV. CONCLUSION

The research work, applying cyber security engineering to aerospace engineering, was carried out using review and explanatory research methods, secondary data, which are online research works in the research area and research fields, with some library materials. The results show that cyber security engineering plays critical roles in the aerospace sector, such as securing communication systems, securing of Data Storage application, ground station security, launch vehicle security, vulnerability management, aerospace supply chain security, etc. From the results, it was concluded that cyber security engineering is very paramount when integrated with aerospace engineering, as it will help to achieve or maintain a secured space segment, a ground segment, and the communication link between the space and the ground segments, including interlinking with other space or ground segments or others in the supply chain.

V. RECOMMENDATION

It is recommended that some various cyber security models or methods for securing each of these segments be investigated and discussed in detail in future work.

REFERENCES

[1]. Ajith Abraham, Crina Grosan, Yuehui Chen (2014): Cyber Security and the Evolution of Intrusion Detection Systems. Pp 1 – 8. https://www.researchgate.net/publication/228641559

[2]. Abel Yeboah-Ofori and Shareeful Islam (2019): Cyber Security Threat Modeling for Supply Chain Organizational Environments. Future Internet, 11, 63; doi:10.3390/fi11030063

[3]. Al-Khasawneh, M. A., Shamsuddin, S. M., Hasan, S., and Bakar, A. A. (2018): An improved chaotic image encryption algorithm. International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-8). IEEE.

[4]. Charalambos Konstantinou, Michail Maniatakos, Fareena Saqiby, Shiyan Huz, Jim Plusquellicx and Yier Jin (2015): Cyber-Physical Systems: A Security Perspective.pp 1-9 https://www.researchgate.net/publication/283228986

[5]. Evan Meyrickab, Aaron Pickarda, Tobias Rahloffa, Sébastien Bonnarta, Antonio Carloa, Kathiravan Thangavel (2021): Ground Station as a Service: A Space Cybersecurity Analysis .72nd International Astronautical Congress (IAC), Dubai, United Arab Emirates, 25-29.

[6]. Felix Ale, Abdullahi Ayegba, Emmanuel Omomoh, GujaharRengje Danlami Rogers, Urukwe Ando, Desmond Wysenyuy, Oyibo Muazu, IruemiOlohimai Juliet and Ndahi Aisha (2024): The role of cybersecurity in remote sensing and geographical information system. International journal of trend in scientific research and Development. Vol 8(4), pp 308-312

[7]. James Pavur and Ivan Martinovic (2022): Building a launch pad for satellite cyber-security research: lessons from 60 years of spaceflight. Journal of Cybersecurity, 2022, pp 1–17. https://doi.org/10.1093/cybsec/tyac008

[8]. Latif M.N.A., Aziz N.A.A., Hussin N.S.N., Aziz Z.A., 2020. Cyber security in supply chain management: asystematic review. LogForum 17 (1), 49-57. http://doi.org/10.17270/J.LOG.2021.555

[9]. Lucas Wallin (2024): Secure Satellite Communication; A system design for cybersecurity in space. Uppsala university, Sweden. UPTEC STS 24034. Pp 13 and 36

[10]. Minwei Peng, Qiang Wei, Rongkuan Ma, Yangyang Geng, Yahui Yang, Shichao Zhang and Yali Zhang (2023): Unauthorized Access Detection for Network Device Firmware WEB Pages. Electronics 2023, 12, 3674. Pp 1- 14. https://doi.org/10.3390/electronics12173674

[11]. Muhammad Ahmad Baballe, Aminu Yau, Sirina Farouk Ibrahim, Bello Abubakar Imam, Mustapha Aliyu, Yusif , Abubakar Sadiq Muhammad, Aliyu Musa Lawan, Abdulmuhamin Muhammad (2023): Management of Vulnerabilities in Cyber Security. Journal of Mathematical techniques and computational mathematics. Vol 2(4), pp 170 – 174

[12]. Sergio Mottini and Luciana Bonino (2016): Optical Links for Fast and Secure Communications on Ground and in Space. https://www.sto.nato.

[13]. Sean Atkinson (2018): “Cybersecurity Tech Basics: Vulnerability management:

Overview". Thomson Reuters. ID: w-013-3774. Pp 1 – 5

[14]. Saqib Ali,Taiseera Al Balushi, Zia Nadir and Omar Khadeer Hussain (2018):Studies in Computational Intelligence. Springer International Publishing. https://doi.org/10.1007/978-3-319-75880-0

[15]. The British Standards Institution (2020): Aerospace Agenda: Information Security. BSI/UK/1678/SC/0120/EN/BLD

[16]. Vinyas D Sagar (2023): Risks and Challenges in the Defence and Aerospace Sector. https://www.researchgate.net/publication/370057543

[17]. what is encryption?,www.cloundfare.com")

[18]. WWW.ibm.com

[19]. www.encyclopedia.com