International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Al-Enabled Predictive Monitoring And Security Systems For Healthcare And Aviation

Aditi Nandiraju , Hunar D, Ashutosh, Somraj, Janaki Kandasamy
Author Details
Aditi Nandiraju
Computer Science & Engineering (AIML)
FET - Jain Deemed-To-Be-University, Bengaluru, India
E-mail: Aditi.nandiraju2@gmail.com
Hunar D
Computer Science & Engineering (CPS)
FET - Jain Deemed-To-Be-University, Bengaluru, India
E-mail: hunarwork11@gmail.com
Ashutosh Rai
Computer Science & Engineering (AIML)
FET - Jain Deemed-To-Be-University, Bengaluru, India
E-mail: JUUG24BTECH15281@jainuniversity.ac.in
Somraj
Computer Science & Engineering (CPS)
FET - Jain Deemed-To-Be-University, Bengaluru, India
E-mail: juug24btech17538@jainuniversity.ac.in
Janaki Kandasamy
Computer Science & Engineering (AI)
FET - Jain Deemed-To-Be-University, Bengaluru, India
E-mail: k.janaki@jainuniversity.ac.in

Abstract- As critical infrastructure in aviation and healthcare becomes increasingly complex, traditional reactive strategies for maintenance and security are proving insufficient for handling dynamic real-world environments. This research examines the integration of AI-enabled predictive monitoring and security frameworks to create resilient, self-sustaining systems that can manage uncertainty with minimal human intervention. Central to this transition is the application of AI and machine learning models—such as XGBoost, CNNs, and LSTMs—to move from scheduled to proactive maintenance by accurately predicting the Remaining Useful Life (RUL) of aircraft engines and providing early warnings for cardiac events in healthcare. Simultaneously, the study prioritizes security by developing defense mechanisms against cyber-physical threats, including GPS spoofing, ADS-B vulnerabilities, and unauthorized network intrusions across both aviation and smart airport infrastructures. Despite these advancements, significant barriers remain, including high computational overhead, a lack of model interpretability (the "black box" problem), and a gap between simulation and real-world deployment. This work concludes that the future of dependable

infrastructure lies in unified, lightweight, and explainable frameworks that allow systems to autonomously detect threats, recover from faults, and maintain themselves in unpredictable conditions.

**Keywords- AI-Enabled Systems, Predictive Maintenance, Cyber-Physical Security,Remaining Useful Life (RUL),Deep Learning,Aviation Infrastructure
,Healthcare Monitoring, Deep Learning.**

I. INTRODUCTION

Unmanned aerial vehicles and modern aircraft have quietly become load-bearing infrastructure. They monitor borders, deliver packages, coordinate disaster relief, and are inching toward carrying passengers autonomously. But as these systems take on more responsibility, keeping them reliable, safe, and efficient has become a genuinely hard problem — one that traditional approaches aren't built to handle.

Fixed control strategies struggle the moment conditions deviate from what they were designed for. Scheduled maintenance is essentially educated guesswork: service the aircraft on a calendar, hope nothing breaks in between. Neither approach holds up well against dynamic environments, unpredictable failures, or the kind of real-time decision-making that modern aerial systems increasingly demand.

Two broad research directions have emerged in response. The first is about control and security — specifically, how to build UAVs that can adapt on the fly using techniques like Model Reference Adaptive Control, while also defending themselves against cyber-physical attacks that could compromise their behavior mid-flight. The second is about maintenance — using AI, machine learning, and IoT sensors to watch aircraft systems continuously, catch signs of degradation early, and predict how much useful life a component has left before it needs attention. Together, these approaches represent a shift from reacting to problems to anticipating them.

The gap, though, is that most research treats these as separate concerns. Control systems are designed in one corner, security mechanisms in another, and maintenance strategies in a third. That siloing makes it difficult to build systems that are truly autonomous and resilient — systems that can detect a fault, adapt their behavior, protect themselves from interference, and make intelligent decisions about when and how to intervene, all at once.

That is the larger ambition driving this work: aerial systems that are not just capable, but self-sustaining — able to manage uncertainty, resist threats, and maintain themselves with minimal human intervention.

II. LITERATURE SURVEY

V. Sharma et al. show that Xgboost optimized ensemble model for remaining useful life prediction of aircraftturbofan engines. This proposes an ensemble ML model which has been optimized using extreme gradient boosting (XGBoost) to predict the remaining useful life (RUL) of aircraft turbofan engines.It is used forfacilitating proactive maintenance, condition monitoring, and diagnosing failures and faults to prevent failures and improve reliability.the system enhances the reliability and robustness of turbofan engines. ML forecasts

potential issues, helping to prevent economic or safety problems. Predictive maintenance well in advance based on RUL prediction can significantly decrease unexpected engine downtime. By optimizing maintenance schedules and preventing catastrophic failures , the system can lead to reduced maintenance expenses. Maintaining engines proactively contributes to better overall asset quality. The use of an XGBoost- optimized ensemble model gives a better approach to RUL prediction, potentially able to lead to higher accuracy ML .models, especially those made better with gradient boosting which can be complex and harder to interpret compared to simpler models. This is a concern in safety-critical applications like aviation. Training and deploying complex ML models can require significant computational resources. The model's performance might depend on the specific engine types andoperating conditions it was trained on, which may limit its generalization to new or different scenarios.[1]

Vikram Sai Prasad Karnam et al. analyze how machine learning (ML) and generative AI (GenAI) can change the

airline industry by improving flight operations and maintenance. The aim is to move from reactive to proactive operational models in aviation. Machine learning and GenAI allow airlines to foresee and solve problems before they become worse and lead to smoother operations using XGBoost, LSTM, Random Forest, Gradient Boosting, and genAI simulation models. These technologies enhance flight scheduling, resource allocation, and maintenance routines. They help reduce costs linked to delays, unexpected repairs, and inefficient operations. By predicting potential failures, these technologies could make flying safer. Airlines which implement these technologies operate better with better service and operational effectiveness. The success of ML and GenAI depends on high -quality, clean and complete data, which could cause challenges in aviation due to various data sources and formats. By integrating new AI systems and older IT infrastructure, it can be complicated and expensive. Bringing in new technologies requires changes in company processes, and employee training. This can be met with resistance. The initial cost of developing, implementing, and maintaining AI solutions is high. The aviation sector is highly regulated, so new technologies must adhere to strict safety and operational requirements, which slow down adoption.[2]

Rupali Rastogi et al. shows how IoT systems used for predictive maintenance of aircraft engines. This one shows the need to ensure reliability and safety of these engines in aerospace engineering. By using sensor data put on aircraft engines and using various techniques like machine learning, deep learning, and hybrid methods, the goal is to predict failures much before they take place . Maintenance can then be planned proactively, which cuts down on unexpected downtime and optimize resource allocation. Preventing unexpected downtime results in significant savings on emergency repairs, operational interruptions, and possible accidents. Using sensor data along with advanced analytical techniques such as ML and DL, it enables more accurate and informed maintenance decisions. Real-time implementation of predictive maintenance strategies involves challenges in data processing, deployment, and quick decision-making in environments. Creating predictive models that stay accurate constantly across different engine types, operating conditions, and failure modes is difficult. Ensuring these models perform well on new data is challenge. Incorporating IoT-based predictive maintenance systems with existing aerospace systems and procedures is complex and takes time. IoT systems are vulnerable to cyber threats, making it crucial to secure sensitive aircraft engine data and control systems.[3]

Lubing Wang et al. focused on improving the aircraft engine maintenance by predicting their Remaining Useful Life (RUL) and using this information to schedule maintenance better . The goal is to monitor engine status in real-time and this reduces maintenance time and allows for continuous tracking. This framework cuts maintenance time by a lot. By using DL and Bayesian optimization, it used data to improve prediction accuracy and scheduling. This framework offers a solution for RUL prediction. The success of this relies a lot on the quality and quantity of historical data available for training the deep learning models. Training and deploying deep learning ensemble models and Bayesian optimization uses a lot of resources. Deep learning models, particularly ensemble ones, act like black boxes which makes it more difficult to interpret their decisions or diagnose problems. The framework's performance could be different when applied to different engine types or whenever operating conditions not included in the training data.[4]

Mingyang Zhou et al. researched how AI was used in monitoring and maintaining aero engine health. It shows the importance for the need for effective monitoring and maintenance for safety, efficiency and resource management in aviation. The research shows AI's advancing in data processing and how it helps in industrial growth. Applying AI in aircraft health monitoring creates automated operation and maintenance systems. This leads to improved flight safety, better efficiency, and cost savings. However, the problem is the lack of large and high quality datasets for aero-engine health monitoring. Datasets like this are needed for training strong and precise AI models that can learn effectively from real-world data. Aero-engine operational data shows complex, non-linear relationships which current AI models might struggle to understand these patterns consistently. Also, there is no unified system for aerospace engine health monitoring and maintenance that can be applied across the aviation industry.[5]

Dydek's work is the most foundational of the five. It's about adaptive control specifically Model Reference Adaptive Control, or MRAC. The idea is straightforward: instead of

fixing control parameters before flight, you keep updating them in real time so the UAV tracks some reference model even as conditions change. The update rule comes from Lyapunov stability theory which matters, because without that, continuously changing parameters mid-flight is actually more dangerous than just using fixed ones.Results show it can handle around 50% variation in system parameters and has some tolerance for actuator failures. For 2010, that's solid.But the tuning dependency is a real problem. Bad gain values and the system either responds too slowly or oscillates. There's also computation cost parameters updating continuously is expensive, which is an issue for smaller UAVs that don't have much onboard processing. And the whole thing assumes you already know the rough structure of your system model. Unknown nonlinear effects don't get handled.Security isn't mentioned at all. Not a criticism exactly just noting the scope. It's a strong foundation for handling physical uncertainty, but nothing beyond that.[6]

This one actually takes security seriously, which, compared to most of the literature, is already notable. The focus is on what happens when someone is actively attacking your UAV GPS spoofing, jamming, false commands injected into the system. Not hypothetical threats.The main contribution is treating the UAV as a cyber-physical system, not just a physical one. Security and control are considered together at the design stage rather than one being bolted onto the other after the fact.The L1 norm is used because it's less sensitive to outliers so if some sensors are feeding corrupted data, the estimate doesn't completely collapse. It degrades, but more gracefully. That only works, though, if the number of compromised sensors stays within limits. If too many are hit simultaneously, it breaks.Formal verification is also used, which gives some provable guarantees rather than just simulation evidence. That's genuinely useful.The computational overhead is real, though. And detection depends on knowing what kinds of attacks to expect not sure how well it handles something novel. Control and security are still somewhat separate conceptually even if they're being considered together. Compared to Dydek, this is clearly addressing a more current threat landscape. But there's still a gap between the framework and something you'd actually deploy.[7]

Aksland et al. reject the standard design sequence build the physical system, then design a controller for it. Co-design optimizes both simultaneously. The argument being that locking one in before the other always leaves performance on the table.The study uses a hybrid electric UAV, so energy management is central. Plant parameters and control inputs are optimized at the same time. The efficiency gains reported are 15 to 25%, which is actually significant. And interestingly, smaller components sometimes beat larger ones not an obvious result.The joint optimization problem is just harder to solve than either sub-problem separately. It also needs an accurate model if your model is off, the 'optimal' solution won't be optimal in practice. And getting different engineering teams to actually coordinate across domains is not as clean in reality as it looks in a paper. Uncertainty and security don't come up at all. It's an efficiency story, design-time only.[8]

This one isn't really about a control method. It's about the development toolchain. The argument is that modeling in one environment, control design in another, and testing in a third causes integration issues and makes moving from simulation to hardware harder than it needs to be.The proposed solution is a single unified platform. Reproducibility improves. The sim-to-real transition is smoother because the testing environment wasn't isolated from the development environment. That's a practical problem worth solving.But simulation fidelity still determines result quality. A unified platform running a bad model is just a more convenient way to get bad results. High-fidelity simulations are computationally expensive. And this paper doesn't introduce new control or security ideas it's infrastructure, not a solution. Still worth including because it addresses a real bottleneck, but I think it gets overstated sometimes.[9]

Wang et al. scale the security problem to swarms multiple UAVs coordinating together. Which is harder in ways that aren't immediately obvious. A single UAV being spoofed is one thing. A swarm where compromised nodes influence other nodes through the coordination mechanism is qualitatively different.Attacks are categorized across levels network (Sybil, wormhole), consensus-level manipulation, formation disruption via Byzantine behavior. Each UAV updates its state based on weighted inputs from neighbors. The system can tolerate some compromised nodes it doesn't immediately collapse but threshold matters a lot and I'm not sure the paper is fully clear on where that threshold sits in realistic scenarios.Machine learning is used for anomaly detection, which makes sense for catching attack patterns that weren't anticipated at design time. The honest issue: almost all results are simulation-based. Real-world swarm

security testing is expensive and logistically hard. Scalability is also unresolved more UAVs means more communication load, and the consensus models don't fully address that. Useful as taxonomy and framework. Far from something deployable.[10]

S. Kumar & et al in their paper "IoT-Based Cardiac Arrest Prediction Using HRV" have proposed a system based on IoT technology that is used for continuous monitoring of heart rate variability and the application of machine learning algorithms for early prediction of cardiac arrest. However, the advantages of the proposed system are that the system makes the use of heart rate variability, which is a good sign of heart health. The system is helpful in making early predictions a few minutes before heart arrest. This is helpful as the person is given an opportunity to survive. IoT technology is used in the development of the system. The system is helpful as the real-time monitoring of the heart rate of the patient is possible with the help of IoT technology. However, the disadvantages of the system are that the accuracy of the system is dependent upon the accuracy of heart sensors. The system is not fully effective for those individuals who have irregular heart rates. The system requires internet connectivity. Output are The developed IoT-based HRV monitoring system was able to predict cardiac arrest a few minutes in advance, High accuracy in the prediction is obtained, Improvement in the generation of early warnings enhanced the chances for survival, Effective real-time Heart remote Rate monitoring was put Variability into place.[11]

Hyeon Hoon Lee and et al propose "Real-Time ECG Analysis for Cardiac Arrest Detection" This paper focuses on the implementation of the "Real Time ECG Monitoring in Intensive Care Units," which utilizes the application of machine learning algorithms for the prediction of cardiac arrest in the hospital setting. This enhances the time response in the event of an emergency. The advantages of the algorithm discussed in the paper include It is implemented for the purpose of "Real Time ECG Data Analysis," which is applicable for decision-making purposes. It has "high reliability" due to the implementation of "short ECG windows," which enhances "timely response/preprocessing time." However, the disadvantages of the algorithm discussed in the paper include It is "mostly suitable for the hospital environment," which is not applicable for "Home Use" due to the "requirement for high-quality clinical ECG equipment," whereas the "implementation cost is high". Output are the real-time ECG analysis model successfully predicted the occurrence of cardiac arrest, Reduced computation delay with short ECG window analysis, Emergency response time was greatly improved, High reliability was observed in the ICU setting.[12]

J. H. Lee, S. M. Lee, and H. K. Yoon discuss "Wearable Sensor-Based Cardiac Monitoring Systems" The authors address the concept of wearable sensor technology for cardiac health monitoring. The paper emphasizes the significance of "continual data acquisition and cloud analysis" to detect abnormal heart conditions at an early stage. The advantages of the Threshold-Based Detection Algorithm are: The mobile technology solution enhances the portability of the equipment. The equipment promotes the early detection of abnormal heart functions. The user interface facilitates the patients. The disadvantages of the Threshold-Based Detection Algorithm are: The precision of the equipment may be low because of the mobile technology. The battery life of mobile devices may be considered a drawback. The equipment lacks the ability to handle complex heart conditions. Output are The result was the early detection of abnormal heart conditions with the use of continuous wearable monitoring, It supported remote patient monitoring with cloud-based analytics,The system improved the accessibility and Signal-to-Noise portability of Ratio cardiac care. [13]

R. Gupta, N. Kumar, and A. Sharma propose "Deep Learning Approaches for Sudden Cardiac Arrest Prediction." The study focuses on the analysis of ECG signals using deep learning technology such as CNN and LSTM. The study suggests better sensitivity and accuracy using these models in comparison to traditional methods. The advantages of this study are: Extensive study of various AI and ML techniques, offering a 360-degree view, Enhancement of the accuracy of the prediction results using traditional techniques, Significance of "big data analytics" in healthcare, Applicability to various hospital monitoring systems and remote monitoring systems. The disadvantages of this study are: The datasets implemented in this study need to be large and diversified, the study might be computationally complex, and The study might be influenced by bias factors based on the training datasets. The output of this study suggests that CNN and LSTM models were found to offer higher sensitivity and accuracy than traditional techniques; ECG signal classification of the

heartbeat using deep learning technology improved prediction results considerably using AI techniques.[14]

S. Aqel and et al. present AI-Driven Early Warning Systems in Healthcare This paper will review some AI-based early warning systems used in healthcare applications and emphasize their predictive analytics for life-threatening conditions like cardiac arrest. Advantages: Enhances the traditional early warning system using ML models; Improves sensitivity and predictive value; Allows early intervention and risk stratification; Can be integrated within prevailing health care systems. Disadvantages: The model performance may degrade with noisy or missing data; Model updating and validation are required regularly; this model may generate false alarms, which increases the alert fatigue. Output are Machine learning-based risk scoring showed better early detection of a life-threatening condition, Predictive analytics for better early interventions, Improved risk stratification in health care monitoring. [15]

Dexter Roberts present Aviation Security and Post-9/11 Reforms This paper presents an overview of the evolution of aviation security policies, especially after the 9/11 incident. In this context, the roles played by government agencies and security policy frameworks, such as the creation of security agencies like the TSA and the implementation of multi-layered security systems, are highlighted as efforts towards preventing terrorism in aviation security. The algorithm used under the THREAT MODELING FRAMEWORK .Advantages: OVERVIEW AVIATION SECURITY EVOLUTION, especially after the 9/11 incident, HIGHLIGHTS THE ROLE PLAYED BY GOVERNMENT AGENCIES, Useful as an academic material, especially when scrutinizing the context and transformations, helps in identifying gaps in conventional security systems. Disadvantages: Gives more emphasis to policy evolution rather than technical implementation, less emphasis is given to contemporary cyber security and AI technologies, Lack of experimental and quantitative analysis. Output are It appears that multi-layered aviation security infrastructures have been bolstered, Models of threat risk assessment enhanced security planning, In addition, there were reforms to the aviation regulations and policies to improve safety systems [16]

R. Ronen and B. BenMoshe present Cyberattack Detection in Flight Systems Using LoRa This paper presents a suggestion for an IoT-based approach for detection and mitigation of cyberattacks within flight systems using LoRa-based IoT technology. Such an approach facilitates the achievement of a real-time network monitoring system for flight systems.The advantages are that it introduces a LoRa-based IoT concept, which is effective in the detection of cyberattacks within the flight system in real time, suitable for long-range communication with reduced power consumption, and improves the continuous monitoring of the flight system's networks. The disadvantages include reduced bandwidth within the LoRa protocol, which might restrict data transmission, requires the installation of more infrastructure, and is not effective when dealing with massive data. The output includes the successful detection of the cyberattack within the LoRa-based intrusion detection system and the achievement of the long-range communication network with reduced power consumption for the continuous monitoring of Packet the network Loss within the Rate aircraft system. [17]

S. Ishtiaq and N. A. Abd Rahman, who wrote article Cybersecurity Vulnerabilities in Aviation Infrastructure In this article, the authors discuss the vulnerabilities in aviation control and communication systems, and various defense mechanisms, including intrusion detection, encryption, and risk mitigation strategies. The advantages of this article are: Identifies vulnerabilities in aviation control and communication systems, Useful for enhancing the cybersecurity of aviation, identifies vulnerabilities in aviation control and communication systems, Useful for enhancing the cybersecurity of aviation, Discusses various defense mechanisms for cybersecurity such as intrusion detection, encryption, etc. The disadvantages of the article are: Only survey-based studies, not all studies relate to AI, Vulnerabilities may be costly for the aviation industry. Output Critical vulnerabilities were identified in aviation control and communication systems, Encryption and intrusion detection of systems were strengthened for security purposes, Risk mitigation strategies were improved for better cybersecurity. [18]

Q. Li and et al present Identifying Risky Pilot Behavior Using Machine Learning This research applies EEG signals and machine learning models to identify risky pilot behaviors under visual flight rules, enhancing proactively aviation safety mechanisms. Advantages Focuses on human factors, which are usually neglected in aviation security, EEG data utilize machine learning for behavioral

analysis. Helps to identify the stress and risky decisions of the pilots. Enhances proactively safety mechanisms. Disadvantages Requires specialized EEG equipment, increasing system complexity Real-time implementation may be challenging. raises issues of privacy and ethics regarding the collection of human data Output EEG-based machine learning models identified risky pilot behavior; Classification accuracy was improved; Human-factor-based risk Classification prediction enhanced aviation safety.[19]

E. Harison and N. Zai Denberg present Cyber Threats in Air Traffic Control and Communication Systems: This survey analyzes cyber threats in air traffic control and aircraft communication systems, particularly in ADS-B vulnerabilities, and highlights secure authentication protocols. Advantages are It gives the critical study of cyber threats in ATC and ADS-B systems; it underlines the vulnerabilities in aircraft communication protocols. It emphasizes that one needs to implement an authentication and encryption mechanism. It is helpful for policy makers and system designers. Disadvantages are Identifies the problem majorly but not the complete solution; the implementation of secure protocols may require coordination all over the world; real-time experimental validation is missing. Output is ADS-B communication vulnerabilities were found out, Emphasized authentication protocols for secure communications, Increased awareness towards cyber risks in ATC systems.[20]

Ash Rossiter Smart Airports and the Evolving Cyber Threat This paper focuses on how smart airports around the globe are vulnerable to cyber threats. This study further describes how terrorists can misuse cybersecurity to attack airport operations. This study also outlines cybersecurity strategies currently used by smart airports. Advantages are This study concentrates on cybersecurity risks faced by smart airports around the globe, Links the threat of terrorism with cyber threats, A good study for gaining more knowledge about cyber threats faced by smart airports around the globe, It gives practical guidance on how to protect smart airport infrastructure from cyber threats. Disadvantages are This study seems to be mainly conceptual, this study can be considered just a theoretical application, although it talks about cybersecurity in smart airports, it has given little emphasis to aircraft cybersecurity, Applying the suggested strategies might require a lot of money to implement. Output are This study emphasized the cyber risk assessment models that exposed vulnerabilities in smart airport infrastructure. This study emphasized the importance of predictive cyber risk analysis in airport digital Cyber security Risk [21]

Shangqing Cao and et al present Robust Management of Airport Security Queues Considering Passenger Non-Compliance This research proposes an optimization-based model to improve airport security screening queues, in particular when passengers do not strictly adhere to the security screening instructions. Such passenger non-compliance may cause security gaps, which could be exploited by attackers. The model improves both efficiency and security as it takes into account unpredictable passenger behavior. Advantages are Addresses human behavior, a major weakness in security systems, improves screening efficiency without reducing security, reduces congestion and operational stress at security checkpoints, Helps minimize vulnerabilities caused by passenger non-compliance. Disadvantages are Based on mathematical and simulation models, not real-world deployment, requires accurate passenger behavior data for best performance, Does not directly address cyber or aircraft system threats. Output are Queue optimization models reduced passenger waiting time, Screening efficiency was improved without reducing security, Passenger non-compliance risks were minimized. [22]

III. CONCLUSION AND FUTURE SCOPE

Looking across the literature, a clear pattern emerges: the field is moving toward systems that are integrated, adaptive, and security-conscious, rather than treating control, maintenance, and protection as separate problems. Data-driven techniques — ensemble learning, XGBoost, deep neural networks — have meaningfully improved how well we can monitor the health of aircraft engines. That progress is real.

But the barriers to actually deploying these systems are just as real. The models that perform best tend to be the most computationally demanding, which creates an immediate tension when the hardware running on a UAV or flight controller has strict power and weight constraints. High-quality, standardized datasets are still hard to come by, which limits how well models trained in one context transfer to another. Most AI systems in this space remain

difficult to interpret — a problem that matters enormously in aviation, where engineers and regulators need to understand not just what a system decided, but why. And a striking amount of the work reviewed here never moves beyond simulation, leaving the gap between lab performance and real-world deployment largely unaddressed.

Closing that gap will require more than incremental improvements to individual techniques. What the field needs are unified, lightweight frameworks that bring control, security, and maintenance together without demanding more compute than the hardware can support. Explainability needs to be treated as a design requirement, not an afterthought, if these systems are ever going to earn the trust of engineers and regulators. Digital twins offer a credible path for stress-testing systems before they fly. Securing IoT infrastructure through blockchain and stronger encryption becomes non-negotiable as more critical systems come online. And longer term, the goal should be systems capable of detecting threats and recovering from faults autonomously, without waiting for human intervention.

Beyond aviation, the same principles carry over into healthcare — where future systems will need to draw on multiple data sources at once, push computation to the edge for faster emergency responses, and layer in multimodal authentication methods like iris scanning and facial recognition to build more robust, situationally aware safety systems. The underlying challenge is the same in both domains: building systems that are not just intelligent in controlled conditions, but dependable in the messy, unpredictable conditions of the real world.

REFERENCES

1. V. Sharma et al., "A XGBoost Optimized Ensemble Model for Remaining Useful Life Prediction Aircraft Turbofan Engines," IEEE https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10472322 Access, 2024.
2. Vikram Sai Prasad Karnam., "Enhancing Flight Operations Using AI-Driven Predictive Maintenance," IEEE Conference on Intelligent Transportation and Aviation Systems, 2023. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10497276
3. Rupali Rastogi et al., "IoT-Based Predictive Maintenance Tactics, Techniques, and Procedures for Aircraft Engines," International Journal of Engineering Research and Technology (IJERT), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10957439 2022.
4. Lubing Wang et al., "Predictive Maintenance Scheduling for Aircraft Engines Based on Remaining Useful Life Prediction," European Journal of Computer Science and Information Technology (EJCSIT), https://eajournals.org/ejcsit/wp-content/uploads/sites/21/2025/05/Enhancing-Flight Operations.pdf 2023.
5. Mingyang Zhou et al., "Research on Aero-Engine Health Monitoring and Maintenance Strategies in the Context of Artificial Intelligence (2019–2024)," IEEE Access, 2024. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10878616&tag=1
6. Z. T. Dydek, Adaptive Control of Unmanned Aerial Systems, Ph.D. dissertation, Massachusetts Institute of Technology, 2010. http://hdl.handle.net/1721.1/62324 [7]M. S. Ale Isaac, P. F. Peña, D. Gîfu, and A. R. Ragab, “Advanced Control Strategies for Securing UAV Systems: A Cyber-Physical Approach,” Sensors, vol. 23, no. 12, pp. 5568, 2023. Advanced Control Strategies for Securing UAV Systems: A Cyber-Physical Approach | Archivo Digital UPM
7. C. T. Aksland, D. L. Clark Jr., C. A. Lupp, and A. G. Alleyne, “Closed-Loop Control and Plant Co-Design of a Hybrid Electric Unmanned Air Vehicle,” ASME J. Dyn. Syst. Meas. Control, vol. 145, no. 8, pp. 081003, 2023. Closed-Loop Control and Plant Co-Design of a Hybrid Electric Unmanned Air Vehicle | J. Dyn. Sys., Meas., Control. | ASME Digital Collection
8. X. Dai, C. Ke, Q. Quan, and K.-Y. Cai, “Unified Simulation and Test Platform for Control Systems of Unmanned Vehicles,” IEEE Trans. Ind. Informat., vol. 12, no. 3, pp. 1243–1252, 2016. ieeexplore.ieee.org/document/10371429
9. X. Wang, Z. Zhao, and L. Yi, “A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures,” ACM Comput. Surveys, vol. 56, no. 11, pp. 1–38, 2024. dblp: A Survey on Security of

UAV Swarm Networks: Attacks and Countermeasures.

10. S. Kumar, U. M. Mohapatra, D. Singh, and D. K. Choubey "IoT- Based Cardiac Arrest Prediction Through Heart Variability Analysis," Advances in Intelligent Systems and Computing, Springer, 2020. Link: https://www.researchgate.net/publication/339669445_IoT-Based_Cardiac_Arrest_Prdiction_Through_Heart_Variability_Analysis
11. Hyeon Hoon Lee, Hyun-Lim Yang, Ho Geol Ryu, Chul-Woo Jung, Youn Joung Cho, Soo Bin Yoon, Hyun-Kyu Yoon & Hyung-Chul Lee "Real-Time Machine Learning Model to Predict In- Hospital Cardiac Arrest Using Heart Rate Variability," npj Digital Medicine, vol. 6, 2023. LINK: https://www.nature.com/articles/s41746-023-00960-2A
12. J. H. Lee, S. M. Lee, and H. K. Yoon " Wearable Sensor-Based Cardiac Monitoring Systems: Review, LINK: https://www.mdpi.com/2079-6374/16/2/93 "Sensors, MDPI, 2021.
13. R. Gupta, N. Kumar, and A. Sharma "Deep Learning-Based Cardiac Arrest Prediction," Mathematics, MDPI, LINK: vol. http://mdpi.com/2227-7390/10/12/2049 10, no. 12, 2022.
14. Sarah Aqel , Sebawe Syaj , Ayah Al-Bzour , Faris Abuzanouneh , Noor Al-Bzour , Jamil Ahmad. "Artificial Intelligence and Machine Learning Applications in Sudden Cardiac Arrest Prediction," 2023. LINK: Current https://pubmed.ncbi.nlm.nih.gov/37792134/ and Cardiology Reports,
15. Dexter Roberts "Aviation Security and the Challenges the Industry Faces Providing Safe Secure LINK: Transportation", ResearchGate, 2017. https://www.researchgate.net/publication/316539988_Aviation_Security_and_the_Challenges_the_Industry_Faces_Providing_Safe_and_Secure_Transportation Using
16. R. Ronen and B. Ben-Moshe, "Cyberattack on Flight Safety: Detection and Mitigation LoRa," LINK: Sensors, vol. https://www.mdpi.com/1424-8220/21/13/4610 21,no. 13, MDPI, 2021.
17. S. Ishtiaq and N. A. Abd Rahman, "Cybersecurity Vulnerabilities and Defence Techniques in Aviation Industry," ICIII 2021. LINK: https://www.researchgate.net/publication/354877223_Cybersecurity_Vulnerabilities_and_Defence_Techniques_in_Aviation_Industry
18. Qinbiao Li, Kam K.H. Ng, Cho Yin Yiu, Xin Yuan, Chun Kiu So, Chun Chung Ho "Securing Air Transportation Safety Through Identifying Pilot's Risky VFR Flying Behaviours," Reliability Engineering & System Safety, 2023. LINK: https://www.sciencedirect.com/science/article/abs/pii/S0951832023003630
19. E. Harison and N. Zai Denberg "Survey of Cyber Threats in Air Traffic Control and Aircraft Communications LINK: Systems, "Springer, 2018. https://www.researchgate.net/publication/324960624_Survey_of_Cyber_Threats_in_Air_Traffic_Control_and_Aircraft_Communications_Systems
20. Ash Rossiter "As the number of air travel passengers exponentially increases every year, airports have evolved as "smart" facilities (i.e., smart airports). Journal of Transportation Security," link: 13 October https://link.springer.com/article/10.1007/s12198-025-00311-0 2025
21. Shangqing Cao, Aparimit Kasliwal, Huangyi Zheng, Masoud Reihanifar, Francesc Robuste, Mark Hansen "This research proposes an optimization-based model to improve airport security screening queues, especially when passengers do not strictly follow link: security instructions" arXiv (Cornell University) 2025 https://arxiv.org/abs/2505.05717