ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

Supporting Pilot Decision-Making in In-Flight Cyber Incidents: A Human-Centered Safety Framework

Imane Ouchen[1]; Mohammed Ben Abdellah[2]

[1,2] Faculty of Legal, Economic and Social Sciences (FSJESO), Mohammed Premier University (UMP), Morocco

Publication Date: 2026/02/18

Abstract: As aircraft systems become increasingly interconnected, cybersecurity has emerged as a critical challenge for aviation safety. While extensive technical and organizational measures protect aeronautical systems, limited attention has been paid to the operational role of pilots when cyber threats occur during flight. Existing training programs emphasize conventional failures and provide limited guidance for managing cyber-related anomalies.

This paper proposes a two-step, human-centered decision-support framework designed to assist pilots in managing in-flight cyber incidents. The approach combines a large language model capable of interpreting natural language descriptions of anomalies with a structured, flowchart-based decision process aligned with aviation procedures. The objective is to support, rather than automate, pilot decision-making under high cognitive workload. Qualitative results from scenario-based simulations with professional pilots indicate improvements in threat identification, decision consistency, and crew coordination. The findings highlight the importance of integrating cybersecurity into pilot training and operational decision-making to enhance human resilience in increasingly digital aviation environments.

Keywords: *Aviation Cybersecurity; Human Factors; Decision Support Systems; Crew Resource Management; In-Flight Cyber Incidents; Safety-Critical Systems.*

How to Cite: Imane Ouchen; Mohammed Ben Abdellah (2026) Supporting Pilot Decision-Making in In-Flight Cyber Incidents: A Human-Centered Safety Framework. *International Journal of Innovative Science and Research Technology*, 11(2), 749-758. https://doi.org/10.38124/ijisrt/26feb495

I. INTRODUCTION

The aviation sector is undergoing a profound digital transformation driven by the increasing integration of advanced avionics, satellite-based navigation systems, and networked communication architectures. While these technologies have significantly enhanced operational efficiency and flight safety, they have simultaneously expanded the cyber-attack surface of modern aircraft. As a result, cybersecurity has emerged as a critical concern for aviation safety, no longer limited to ground-based infrastructures or organizational information systems, but extending directly into the cockpit environment.

Recent studies and incident reports have highlighted the growing plausibility of cyber threats affecting airborne systems, particularly those relying on Global Navigation Satellite Systems (GNSS). Attacks such as GPS jamming and spoofing have demonstrated the potential to degrade navigation accuracy or provide misleading information while maintaining apparently coherent system parameters. Beyond navigation, cyber-induced anomalies may also affect avionics displays, data integrity, or communication systems, often presenting symptoms that closely resemble conventional technical failures. This ambiguity significantly complicates in-flight diagnosis and response.

Despite substantial investments in technical and organizational cybersecurity measures by manufacturers, operators, and regulatory authorities, the operational role of flight crews in managing cyber-related events remains insufficiently addressed. Pilot training programs are traditionally focused on mechanical failures, environmental hazards, and procedural emergencies, with little explicit

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

consideration given to cyber-originated anomalies. Consequently, pilots may lack the cognitive frameworks and decision-support mechanisms required to recognize and manage cyber threats under high workload and time pressure.

Importantly, addressing this gap does not imply transforming pilots into cybersecurity specialists. Instead, it requires providing them with operationally relevant tools that support situation awareness, reduce uncertainty, and structure decision-making in ambiguous contexts. Aviation has long relied on standardized procedures, checklists, and decision flowcharts to mitigate human error and enhance safety in abnormal situations. These principles, deeply embedded in Crew Resource Management (CRM) practices, offer a robust foundation for integrating cybersecurity into flight operations.

In parallel, recent advances in artificial intelligence, particularly large language models (LLMs), have opened new perspectives for human-centered decision support. LLMs demonstrate strong capabilities in interpreting natural language inputs, identifying patterns, and synthesizing complex information. When appropriately constrained and combined with established operational procedures, such models may serve as cognitive support tools rather than autonomous decision-makers, thereby preserving human authority and responsibility.

This paper proposes a two-step decision-support framework designed to assist pilots in managing in-flight cyber incidents. The first step relies on a large language model capable of analyzing natural language descriptions provided by pilots when anomalies are observed, enabling an initial qualification of the situation as: (i) a probable GNSS-related attack (jamming or spoofing), (ii) a cyberattack affecting other onboard systems, or (iii) an event with no apparent cyber origin. The second step consists of a structured flowchart-based decision process aligned with existing aviation procedures, guiding pilots through a sequence of operationally actionable questions and responses.

The objective of this framework is not to automate pilot decision-making, but to support it under conditions of high cognitive load. By combining artificial intelligence with proven procedural approaches, the proposed system aims to enhance threat identification, improve operational consistency, and reinforce human resilience within the aviation system.

This study makes three main contributions. First, it addresses a critical gap in the literature by explicitly focusing on the pilot's role in in-flight cybersecurity management. Second, it introduces a human-centered decision-support framework that integrates LLM capabilities with aviation-standard procedures. Third, it provides qualitative insights into the potential operational benefits of such an approach in terms of situation awareness, decision speed, and workload management.

II. LITERATURE REVIEW

- *Aviation Cybersecurity and Emerging In-Flight Threats*

The increasing digitalization of modern aircraft has fundamentally transformed aviation into a complex cyber-physical system. Advanced avionics, satellite-based navigation, data-link communications, and automated flight management systems are now tightly interconnected, enabling unprecedented levels of operational efficiency and situational awareness. However, this technological integration has also expanded the potential cyber-attack surface of aircraft, raising concerns regarding the resilience of airborne systems to malicious interference.

Existing literature identifies Global Navigation Satellite Systems (GNSS) as one of the most exposed components of aviation infrastructure. GPS jamming and spoofing attacks have been extensively documented in both civil and military contexts, demonstrating their ability to degrade navigation performance or provide misleading positional information while preserving apparently coherent system outputs. Unlike conventional equipment failures, these attacks may not immediately trigger system alerts, thereby delaying detection and increasing the risk of inappropriate pilot responses.

Beyond navigation systems, researchers have highlighted the potential vulnerability of other onboard systems, including avionics data buses, flight management systems, and communication interfaces. Cyber-induced anomalies affecting these components may manifest as inconsistent displays, intermittent system behavior, or abnormal alerts that closely resemble technical malfunctions. This ambiguity complicates in-flight diagnosis and challenges established fault-management paradigms.

Despite these identified risks, the majority of aviation cybersecurity research remains focused on technical safeguards, certification processes, and organizational governance. While these dimensions are essential, they provide limited insight into how cyber incidents may be managed operationally once an aircraft is airborne, where time pressure, workload, and safety constraints severely limit available response options.

- *Human Factors, Pilot Training, and Abnormal Situation Management*

Human factors have long been recognized as a cornerstone of aviation safety. Extensive research has demonstrated that pilot decision-making, situation awareness, and crew coordination play a decisive role in managing abnormal and emergency situations. Training programs emphasize structured responses to engine failures, system degradations, weather hazards, and other well-characterized threats through standardized procedures and simulator-based practice.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

However, several studies point to a growing mismatch between the nature of emerging cyber threats and the scope of current pilot training. While pilots are highly proficient in diagnosing mechanical failures and following predefined checklists, they are rarely exposed to scenarios involving cyber-originated anomalies. As a result, cyber events may be misinterpreted as conventional failures, leading to delayed or suboptimal responses.

Crew Resource Management (CRM) research further indicates that ambiguous situations increase cognitive workload, heighten stress, and exacerbate decision-making biases such as confirmation bias or over-reliance on automation. In the context of cyber incidents, these factors may impair the crew's ability to collectively assess the situation, share weak signals, and adapt strategies in a timely manner. The absence of explicit cyber-related cognitive frameworks within CRM training represents a significant gap in current safety practices.

Recent work in safety science emphasizes that effective training for novel threats does not necessarily require extensive technical expertise. Instead, it relies on providing operators with simplified mental models, decision cues, and structured reasoning processes that support sense-making under uncertainty. This perspective aligns with the aviation tradition of prioritizing operational robustness over technical depth in cockpit training.

- *Decision-Support Systems and Artificial Intelligence in Aviation*

Decision-support systems have been used in aviation for decades to enhance human performance and mitigate error. Flowcharts, checklists, and procedural guidance tools have proven effective in reducing ambiguity, standardizing responses, and maintaining safety margins during abnormal operations. Their success lies in their ability to structure human reasoning without removing decision authority from the pilot.

More recently, advances in artificial intelligence have led to increasing interest in AI-based decision support within safety-critical domains. Large language models (LLMs), in particular, have demonstrated strong capabilities in processing natural language, identifying patterns across heterogeneous information sources, and generating context-relevant interpretations.

In aviation, these capabilities open new possibilities for supporting pilots when facing poorly structured or unfamiliar situations.

Nevertheless, the literature consistently cautions against excessive automation in high-risk environments. Fully autonomous decision-making systems raise concerns related to transparency, trust, certification, and accountability. Consequently, a growing body of research advocates for human-centered AI approaches, where artificial intelligence augments human cognition rather than replacing it.

Within this framework, combining AI-based interpretation with established procedural decision tools appears particularly promising. By using AI to reduce initial ambiguity and guide attention, and procedural structures to ensure operational consistency, such hybrid systems may offer an effective balance between innovation and safety. However, empirical studies examining this approach in the specific context of in-flight cybersecurity remain scarce.

- *Identified Research Gap*

The literature review reveals a clear gap at the intersection of aviation cybersecurity, human factors, and operational decision-making. While cyber threats to airborne systems are increasingly acknowledged, and while human performance in abnormal situations is well studied, few works explicitly address how pilots should be supported when cyber incidents occur during flight.

In particular, there is a lack of research focusing on decision-support frameworks that are both cyber-aware and operationally compatible with existing aviation practices. The absence of such frameworks limits the ability of pilots to effectively manage cyber-related events and undermines the overall resilience of the aviation system.

This study addresses this gap by proposing and evaluating a human-centered decision-support framework that integrates large language model capabilities with structured, aviation-standard decision processes, specifically designed for in-flight cyber incident management.

III. THEORETICAL FRAMEWORK AND HYPOTHESES

- *Conceptual Foundations*

The proposed research is grounded in three complementary theoretical foundations: situation awareness theory, human-centered decision-making in safety-critical systems, and the principles of Crew Resource Management (CRM). Together, these frameworks provide a coherent basis for analyzing pilot behavior when confronted with cyber-induced anomalies during flight.

Situation awareness theory describes operator performance as a three-level cognitive process involving perception of relevant cues, comprehension of their meaning, and projection of future system states. In the context of in-flight cyber incidents, this process is particularly challenged by the ambiguous and often deceptive nature of cyber-induced symptoms. Unlike conventional technical failures, cyber events may produce signals that appear plausible and internally consistent, thereby delaying recognition and impairing sense-making.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

Human-centered decision-making research further emphasizes that operator performance degrades when uncertainty, time pressure, and cognitive workload increase simultaneously. In such conditions, decision-makers tend to rely on heuristics, prior experience, or automation outputs, which may not be well suited to novel threat categories such as cyberattacks. Consequently, decision-support mechanisms that structure reasoning and reduce ambiguity are critical for maintaining safety margins.

Crew Resource Management provides an operational framework for translating these cognitive principles into aviation practice. CRM emphasizes communication, shared situation awareness, leadership, and coordinated decision-making under stress. However, existing CRM training largely focuses on conventional threats and does not explicitly address cyber-originated events. This gap suggests the need for cyber-aware extensions of CRM principles that preserve their human-centered orientation.

➢ *Cyber Incidents as a New Class of Abnormal Situations*

From an operational perspective, in-flight cyber incidents can be conceptualized as a distinct class of abnormal situations. While they may manifest through technical symptoms, their underlying causes, dynamics, and appropriate responses differ from those of traditional failures. In particular, cyber incidents are characterized by:

- ambiguous and evolving symptom patterns,
- potential deception rather than degradation,
- limited observability of root causes,
- and high dependence on operator interpretation.

These characteristics challenge established fault-management strategies, which typically rely on deterministic cause–effect relationships and predefined procedural paths. Without explicit cognitive and procedural support, pilots may misclassify cyber incidents as technical malfunctions, leading to inappropriate actions or delayed responses.

Accordingly, effective management of cyber incidents requires support mechanisms that enhance early detection, facilitate correct interpretation, and guide adaptive decision-making while maintaining pilot authority and responsibility.

➢ *Human-Centered Decision-Support Framework*

The theoretical framework underlying this study assumes that decision-support systems can enhance pilot performance if they are designed to augment, rather than replace, human cognition. In line with human-centered AI principles, the proposed framework combines two complementary components.

The first component is an artificial intelligence–based interpretive layer, implemented through a large language model. Its role is to assist pilots in transforming natural language descriptions of observed anomalies into an initial situational qualification. By aggregating weak signals and contextual cues, this component aims to reduce ambiguity at the earliest stage of the decision process.

The second component is a structured, flowchart-based decision process aligned with aviation-standard procedures. This component guides pilots through a sequence of binary decision points leading to operationally actionable outcomes. Importantly, this structure preserves the logic of existing checklists and abnormal procedures, ensuring compatibility with established training and certification practices.

The interaction between these components is designed to support the three levels of situation awareness: perception (through anomaly description), comprehension (through AI-assisted qualification), and projection (through structured decision pathways).

➢ *Research Hypotheses*

Based on the theoretical framework described above, this study formulates two primary hypotheses.

- *H1:*

Pilots supported by the proposed decision-support framework will demonstrate improved detection and identification of cyber-originated anomalies compared to pilots relying solely on standard procedures and generic competencies.

- *H2:*

Pilots using the decision-support framework will exhibit more consistent and timely decision-making under cyber-incident scenarios, as reflected by reduced uncertainty, improved crew coordination, and clearer operational responses.

These hypotheses are grounded in the assumption that structured cognitive support enhances situation awareness and mitigates the adverse effects of uncertainty and workload in safety-critical environments.

➢ *Operationalization of Performance Assessment*

To evaluate these hypotheses, pilot performance is assessed across three sequential stages of situation awareness:

- Detection of abnormal behavior,
- Identification and interpretation of the event's nature and consequences,
- Development of an adaptive response strategy and decision.

Performance is measured using both quantitative indicators (e.g., reaction time, decision latency, interaction patterns) and qualitative indicators (e.g., clarity of situation assessment, crew consensus, procedural coherence). This mixed approach reflects the complex and context-dependent nature of human performance in cyber-related flight scenarios.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

IV. METHODOLOGY

➢ *Research Design*

This study adopts a qualitative, scenario-based experimental design aimed at examining pilot decision-making when confronted with in-flight cyber incidents. Given the exploratory nature of the research and the limited availability of trained flight crews, the study focuses on identifying behavioral patterns, decision processes, and situational awareness dynamics rather than achieving statistical generalization.

A comparative approach is employed, involving two groups of flight crews exposed to identical simulated flight scenarios incorporating cyber-induced anomalies. One group operates with standard procedures and generic competencies, while the other group is supported by the proposed two-step decision-support framework.

This design allows for a controlled examination of the impact of cyber-specific decision support on pilot performance under comparable operational conditions.

➢ *Participants*

The study involves professional airline pilots with operational experience on short-, medium-, and long-haul aircraft. Participants are divided into two groups:

- A control group, relying on standard operating procedures (SOPs), conventional abnormal procedures, and generic Crew Resource Management (CRM) competencies;
- A test group, provided with access to the proposed decision-support framework prior to the simulation sessions.

All participants hold valid licenses and are actively engaged in line operations. To ensure comparability, both groups are balanced in terms of flight experience, aircraft category familiarity, and crew composition. Participation is voluntary, and all data are anonymized to ensure confidentiality.

➢ *Simulation Environment and Scenarios*

The experimental sessions are conducted using a certified flight simulation environment representative of modern commercial aircraft cockpits. The simulator reproduces standard avionics interfaces, navigation displays, and flight management systems consistent with current operational configurations.

Each crew is exposed to a set of predefined flight scenarios that include cyber-induced anomalies embedded within otherwise nominal flight profiles. These scenarios are designed to reflect realistic operational contexts and are structured to ensure repeatability across crews.

The cyber scenarios fall into three categories:

- GNSS-related attacks, including GPS jamming and spoofing, characterized by degraded or misleading navigation information;
- Non-GNSS cyber anomalies, affecting avionics or communication systems through inconsistent or erratic behavior;
- Baseline anomalies, with no cyber origin, serving as control conditions.

The scenarios are introduced without prior indication of their cyber nature, requiring pilots to rely on observed symptoms and operational judgment.

➢ *Decision-Support Framework Implementation*

The proposed decision-support framework consists of two sequential components.

The first component is an AI-based interpretive module implemented through a large language model. During the simulation, pilots are able to provide natural language descriptions of observed anomalies. The model processes these inputs and returns an initial qualification of the situation, categorizing it as a probable GNSS-related cyberattack, a cyberattack affecting other onboard systems, or an event with no apparent cyber origin.

The second component is a structured, flowchart-based decision process aligned with aviation-standard procedures. Based on the initial qualification, pilots follow a series of binary (yes/no) decision points leading to operationally actionable guidance. This component is designed to be consistent with existing checklists and abnormal procedures, ensuring procedural familiarity and minimizing training overhead.

The framework is presented as a decision-support aid and does not issue autonomous commands or override pilot authority.

➢ *Data Collection*

Data are collected throughout the simulation sessions using multiple complementary methods.

Quantitative data include:

- Time to initial anomaly detection,
- Time to situation qualification,
- Time to decision implementation,
- Frequency and sequencing of crew interactions.

Qualitative data include:

- Verbal protocols and crew communications,
- Clarity and coherence of situation assessments,
- Level of crew consensus during decision-making,
- Post-simulation debriefing interviews.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

All sessions are recorded and transcribed to enable detailed behavioral analysis.

➢ *Performance Assessment Criteria*

Pilot performance is evaluated according to the three stages of situation awareness:

- Detection of abnormal system behavior,
- Identification and interpretation of the anomaly's nature and potential consequences,
- Development and execution of an adaptive response strategy.

For each stage, performance indicators are defined a priori and applied consistently across all crews. This structured assessment approach ensures traceability between observed behaviors, analytical categories, and research hypotheses.

➢ *Data Analysis Approach*

Given the qualitative focus of the study, data analysis emphasizes pattern identification and cross-case comparison rather than statistical inference. Quantitative indicators are used descriptively to support qualitative findings and highlight observable trends between the control and test groups.

Qualitative data are analyzed using thematic analysis, focusing on decision rationale, communication dynamics, and procedural adherence. Triangulation across data sources enhances the robustness of the findings and supports the validity of the interpretations.

V. RESULTS

➢ *Detection of Abnormal Situations*

Across all simulation sessions, both control and test groups successfully detected the presence of abnormal system behavior during the flight scenarios. However, notable differences were observed in the timing and manner of detection.

Crews in the test group generally identified anomalies at an earlier stage of their manifestation, often during the initial appearance of weak or inconsistent cues. These cues included minor navigation discrepancies, intermittent system alerts, or subtle inconsistencies between displayed parameters. In contrast, crews in the control group tended to wait for more explicit system degradations or alert messages before acknowledging the presence of an abnormal situation.

Quantitatively, the time elapsed between the onset of the anomaly and verbal recognition by the crew was consistently shorter for the test group. Additionally, test group crews more frequently initiated cross-checks and verbal confirmations during this early phase, whereas control group crews often focused on single-system interpretations.

➢ *Identification and Interpretation of the Anomaly*

Differences between groups became more pronounced during the identification and interpretation phase. Crews using the decision-support framework were more likely to explicitly consider a cyber-related origin when describing the anomaly. Their verbal protocols included references to potential deception, signal inconsistency, or system behavior that appeared plausible yet contradictory.

In GNSS-related scenarios, test group crews more frequently distinguished between signal degradation and misleading but coherent navigation data. They articulated uncertainty regarding the integrity of the information rather than assuming a conventional sensor failure. Conversely, control group crews predominantly framed these situations as standard navigation malfunctions, often attempting to reconcile discrepancies within existing technical fault models.

For non-GNSS cyber scenarios, test group crews demonstrated greater consistency in identifying abnormal patterns across multiple systems. Control group crews, by comparison, exhibited a higher degree of fragmentation in their interpretations, with differing hypotheses emerging between crew members and limited convergence during the identification phase.

➢ *Decision-Making and Response Strategies*

During the decision-making stage, test group crews exhibited more structured and coherent response strategies. Their decisions followed clearer logical sequences, with explicit links between observed cues, situational interpretation, and selected actions. The use of the flowchart-based decision process resulted in more uniform response patterns across different crews facing identical scenarios.

Control group crews showed greater variability in decision paths. In several cases, decision-making involved trial-and-error adjustments, prolonged discussions, or sequential reversals of previously selected actions. This variability was particularly evident in scenarios where system behavior remained internally consistent despite being misleading.

In terms of timing, the duration between situation qualification and action implementation was shorter for the test group. Crew communications during this phase were more concise and task-oriented, with clearer task allocation and confirmation of responsibilities.

➢ *Crew Coordination and Communication*

Analysis of crew interactions revealed distinct communication patterns between the two groups. Test group crews demonstrated higher levels of explicit information sharing, including verbalization of uncertainty and solicitation of confirmation from the other pilot. These crews more frequently achieved early consensus regarding the nature of the situation and the intended course of action.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

In contrast, control group crews occasionally exhibited parallel reasoning processes, with each pilot pursuing independent interpretations before converging on a shared understanding. This delayed convergence was sometimes accompanied by increased communication load and overlapping exchanges.

Post-simulation debriefings indicated that test group crews perceived a clearer shared mental model during cyber-related scenarios, whereas control group crews reported greater ambiguity and uncertainty.

➢ *Summary of Observed Performance Differences*

Overall, the results indicate consistent differences between the control and test groups across all three stages of situation awareness. The test group demonstrated earlier detection, more accurate and consistent interpretation, and more structured decision-making in the presence of cyber-induced anomalies.

These observations were consistent across GNSS-related and non-GNSS cyber scenarios, as well as across different levels of crew experience. No instances were observed in which the use of the decision-support framework led to inappropriate or unsafe actions.

VI. DISCUSSION

➢ *Interpretation of Key Findings*

The results of this study highlight clear differences in how flight crews detect, interpret, and manage cyber-induced anomalies when supported by a dedicated decision-support framework. While both control and test groups were able to recognize abnormal situations, the test group consistently demonstrated earlier detection, more coherent interpretation, and more structured decision-making.

These findings suggest that cyber incidents introduce a form of operational ambiguity that is not adequately addressed by conventional training or standard procedures alone. In the absence of explicit cyber-related cues, pilots relying solely on traditional fault-management paradigms tend to frame anomalies within familiar technical models. This behavior is consistent with previous research on sense-making under uncertainty, which shows that operators often interpret novel situations through existing mental schemas.

By contrast, the decision-support framework appears to facilitate an earlier shift from symptom-based reasoning to integrity-based reasoning. Rather than attempting to reconcile inconsistent data within a purely technical fault model, test group crews more frequently questioned the reliability of the information itself. This shift is particularly relevant in the context of cyber threats, where deception rather than degradation may be the defining characteristic.

➢ *Implications for Situation Awareness and Decision-Making*

The observed improvements across the three stages of situation awareness—detection, comprehension, and response—support the theoretical assumption that structured cognitive support enhances operator performance in safety-critical environments. The integration of a large language model at the initial stage of the decision process appears to reduce ambiguity by aggregating weak signals and guiding attention toward relevant threat categories.

Importantly, this support does not replace human judgment. Instead, it acts as a catalyst for collective reasoning within the cockpit, encouraging explicit communication, hypothesis sharing, and early consensus. These behaviors are central to effective Crew Resource Management and have been repeatedly associated with improved safety outcomes.

The flowchart-based decision component further contributes to operational consistency by providing a familiar procedural structure. This alignment with existing aviation practices likely explains why the framework did not introduce unsafe behaviors or excessive reliance on automation. Rather than bypassing established procedures, it complements them by addressing a gap that current checklists do not explicitly cover.

➢ *Contribution to Aviation Cybersecurity and Human Factors Research*

This study contributes to the existing literature in several ways. First, it explicitly positions pilots as active agents in aviation cybersecurity, rather than passive recipients of technical protections. While much of the current research focuses on system-level defenses and certification processes, the present findings underscore the importance of human resilience once an aircraft is airborne.

Second, the study demonstrates the feasibility of integrating artificial intelligence into cockpit decision-making in a human-centered manner. By constraining the role of the LLM to interpretation and classification, and by embedding its outputs within procedural decision tools, the framework avoids many of the concerns associated with autonomous AI systems in safety-critical domains.

Third, the results extend Crew Resource Management concepts into the cyber domain. The observed improvements in communication, shared situation awareness, and coordinated action suggest that cybersecurity can be meaningfully incorporated into CRM without fundamentally altering its principles. This extension aligns with broader trends in safety science that emphasize adaptability and resilience in the face of emerging threats.

➢ *Operational and Training Implications*

From an operational perspective, the findings suggest that pilots can benefit from cyber-specific decision support without requiring extensive technical training. The framework

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

leverages existing cognitive skills and procedural habits, making it compatible with current training philosophies and certification constraints.

In terms of training, the results support the inclusion of cyber-related scenarios in simulator sessions. Exposure to ambiguous, deception-based events may help crews develop the reflexes and communication strategies necessary to manage such situations effectively. The use of decision-support tools during training could further reinforce appropriate reasoning patterns and reduce the likelihood of misclassification during real-world operations.

These implications are consistent with international recommendations encouraging role-based cybersecurity training across the aviation sector. By focusing on operational decision-making rather than technical detail, the proposed approach offers a pragmatic pathway for enhancing cyber resilience at the cockpit level.

➢ *Limitations of the Study*

Several limitations must be acknowledged. First, the qualitative nature of the study and the limited number of participating crews restrict the generalizability of the findings. While the observed patterns are consistent and robust across scenarios, they should be interpreted as indicative rather than definitive.

Second, the simulation environment, although representative, cannot fully capture the stress and contextual complexity of real-world flight operations. Actual cyber incidents may involve additional constraints, including external communications, operational pressures, and organizational factors not addressed in this study.

Third, the large language model used in the framework was evaluated as a decision-support aid rather than as a certified avionics component. Issues related to certification, verification, and long-term trust calibration remain beyond the scope of the present work and warrant further investigation.

➢ *Directions for Future Research*

Future research should aim to validate the proposed framework at a larger scale, incorporating a broader range of aircraft types, operational contexts, and crew compositions. Quantitative studies could complement the present qualitative findings by examining performance metrics across extended training programs.

Additional work is also needed to explore certification pathways for AI-assisted decision-support tools in aviation, as well as their integration with existing safety management systems. Finally, longitudinal studies could assess how repeated exposure to cyber scenarios influences pilot confidence, adaptability, and long-term decision-making behavior.

VII. CONCLUSION AND IMPLICATIONS

➢ *Summary of Findings*

This study examined the role of pilots in managing in-flight cyber incidents and evaluated a human-centered decision-support framework combining a large language model with structured, flowchart-based procedures. The results demonstrate that cyber-induced anomalies constitute a distinct class of abnormal situations that challenge conventional fault-management strategies.

Crews supported by the proposed framework exhibited earlier detection of anomalies, more coherent interpretation of ambiguous system behavior, and more structured decision-making under conditions of uncertainty. These improvements were observed across both GNSS-related attacks and non-GNSS cyber scenarios, without introducing unsafe behaviors or excessive reliance on automation.

Overall, the findings confirm that cyber resilience in aviation cannot rely solely on technical safeguards. Human performance, particularly at the cockpit level, remains a critical factor once an aircraft is airborne and exposed to ambiguous or deceptive system behavior.

➢ *Theoretical Implications*

From a theoretical perspective, this research contributes to the intersection of aviation cybersecurity, human factors, and decision-making in safety-critical systems. It extends situation awareness theory by illustrating how cyber threats disrupt traditional perception–comprehension–projection processes through deception rather than degradation.

The study also reinforces the relevance of human-centered AI principles in aviation. By constraining artificial intelligence to an interpretive and supportive role, and embedding it within established procedural structures, the proposed framework demonstrates how AI can enhance cognitive resilience without undermining human authority or accountability.

Furthermore, the findings suggest that Crew Resource Management concepts can be meaningfully extended to the cyber domain. Cyber incidents amplify the importance of communication, shared mental models, and coordinated reasoning, reinforcing the centrality of CRM as a foundation for managing emerging threats.

➢ *Practical and Operational Implications*

At an operational level, the results indicate that pilots can be effectively supported in managing cyber incidents without requiring extensive technical cybersecurity training. Decision-support tools that align with existing procedures and cognitive habits offer a pragmatic approach to addressing the growing complexity of digital flight environments.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

For training organizations and operators, the study supports the integration of cyber-related scenarios into simulator training programs. Such scenarios can help crews develop appropriate reasoning strategies, improve situation awareness under ambiguity, and reinforce effective crew coordination. Importantly, this integration can be achieved within current training philosophies, minimizing additional burden on training curricula.

From a regulatory and organizational standpoint, the findings align with international initiatives promoting role-based cybersecurity awareness. Positioning pilots as active contributors to cyber resilience strengthens the overall safety system and complements existing technical and organizational defenses.

➢ *Limitations And Future Perspectives*

While the results are encouraging, several limitations must be acknowledged. The exploratory and qualitative nature of the study limits statistical generalization, and the simulation environment cannot fully replicate the complexity of real-world operations. In addition, the certification and long-term integration of AI-based decision-support tools in the cockpit remain open challenges.

Future research should focus on large-scale validation studies, quantitative performance assessment, and longitudinal evaluations of training effectiveness. Further work is also required to explore certification pathways and governance models for AI-assisted decision support in aviation, ensuring transparency, trust, and regulatory compliance.

➢ *Final Remarks*

As aviation systems continue to evolve toward greater digital integration, cyber threats will increasingly intersect with operational decision-making. This study demonstrates that addressing these challenges requires not only technical solutions, but also a renewed focus on human resilience and cognitive support.

By integrating cybersecurity into pilot decision-making frameworks and training practices, the aviation community can strengthen its ability to manage emerging risks while preserving the principles that have long underpinned flight safety. In this sense, cybersecurity should be viewed not as an external constraint, but as an integral component of modern airmanship in an increasingly connected aviation environment.

RÉFÉRENCES

➢ *Aviation Cybersecurity & GNSS Threats*

[1]. Kerns, A.J., Shepard, D.P., Bhatti, J.A., Humphreys, T.E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, 31(4), 617–636.

[2]. Humphreys, T.E. (2019). Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 55(2), 933–946.

[3]. McCallie, D., Butts, J., Mills, R. (2011). Security analysis of the ADS-B implementation. *International Journal of Critical Infrastructure Protection*, 4(2), 78–87.

[4]. Sampson, R., Smith, J. (2020). Cyber threats to civil aviation: Emerging risks and mitigation strategies. *Aerospace*, 7(10), 145.

➢ *Human factors, CRM & Situation Awareness*

[5]. Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32–64.

[6]. Salmon, P.M., Stanton, N.A., Walker, G.H. (2018). Situation awareness measurement: A review. *Safety Science*, 105, 238–247.

[7]. Flin, R., O'Connor, P., Crichton, M. (2008). *Safety at the sharp end: A guide to non-technical skills*. Ashgate.

[8]. Helmreich, R.L., Merritt, A.C. (2017). *Culture at work in aviation and medicine*. Routledge.

[9]. Dekker, S. (2014). *The Field Guide to Human Error*. CRC Press.

➢ *Decision-Making Under Uncertainty & Safety Science*

[10]. Hollnagel, E. (2018). *Safety-I and Safety-II: The past and future of safety management*. Ashgate.

[11]. Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.

[12]. Woods, D.D., Hollnagel, E. (2006). Joint cognitive systems: Patterns in cognitive systems engineering. CRC Press.

➢ *AI & Decision-Support Systems (Human-Centered AI)*

[13]. Amershi, S., et al. (2019). Guidelines for human-AI interaction. *Proceedings of CHI*, ACM.

[14]. Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human–Computer Interaction*, 36(6), 495–504.

[15]. Rahwan, I., et al. (2019). Machine behaviour. *Nature*, 568, 477–486.

[16]. Gunning, D., Aha, D. (2019). DARPA's Explainable Artificial Intelligence (XAI) program. *AI Magazine*, 40(2), 44–58.

➢ *Aviation Decision-Support & Cyber-Physical Systems*

[17]. Kontogiannis, T. (2021). Safety and resilience engineering in aviation. *Safety Science*, 134, 105050.

[18]. Li, W.C., Harris, D., Yu, C.S. (2008). Routes to failure: Analysis of 41 civil aviation accidents. *Accident Analysis & Prevention*, 40(2), 426–434.

[19]. Kopardekar, P., et al. (2016). Unmanned aircraft system traffic management (UTM). *NASA Technical Report*.

[20]. Man, Y., et al. (2020). Cyber-physical systems safety: A systematic review. *Reliability Engineering & System Safety*, 202, 107055.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb495

➢ *Cyber Resilience & Training*

[21]. Linkov, I., Trump, B.D. (2019). *The science and practice of resilience*. Springer.

[22]. Boyes, H., Isbell, R., Watson, T. (2021). Cybersecurity for safety-critical systems. *Safety*, 7(2), 35.

[23]. ICAO (2022). *Cybersecurity in civil aviation*. ICAO Doc 9985.