Human Factors in Cybersecurity, Vol. 168, 2025, 100–110
https://doi.org/10.54941/ahfe1006147

Investigating Human Factors Engineering Integration in ATC Cybersecurity Resilience

Hui Wang and Nathan Royal Schultz

Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA

ABSTRACT

The digital transformation of Air Traffic Control (ATC) has enhanced system efficiency and safety but introduced cybersecurity vulnerabilities. Current cyber defense solutions often overlook the role of air traffic controllers (ATCOs), the primary users of the technology. Human factors issues, such as cognitive overload and reduced situational awareness during cyber incidents, can diminish the effectiveness of human-machine performance and compromise operational safety. This study proposes integrating Human Factors Engineering (HFE) into ATC cybersecurity to optimize human-system interaction. Using an exploratory qualitative approach, it draws from literature, government reports, case studies, and industry practices to develop a conceptual framework. Five HFE principles—user-centered design, error reduction, safety prioritization, individual differences, and task-person fit—are identified as vital. Finally, this study highlights the need for a human-centered cybersecurity approach that strengthens both technological and human resilience, laying the foundation for future research on HFE's measurable impact in ATC environments.

Keywords: Air traffic control, Cybersecurity, Human factors engineering, Human-system interaction, Safety

INTRODUCTION

The integration of computer technology in aviation has significantly enhanced air traffic management (ATM), improving safety and efficiency (Pereira et al., 2022). Next Generation Air Transportation System (NextGen) initiatives have advanced capabilities in communication, navigation, and surveillance, helping air traffic controllers (ATCOs) manage workloads and maintain situational awareness (SA) (Elmarady & Rahouma, 2021). Over the past several decades, ATC infrastructure has evolved from reliance on voice communication and ground-based radar to the use of automated decision-support tools, satellite navigation, and data link technologies (Hird, 2021). While this modernization has streamlined operations and improved capacity, it has also introduced new digital dependencies.

As digital infrastructure becomes central to ATM operations, the system faces growing cybersecurity risks. These threats can compromise system integrity and disrupt air traffic control (ATC), as seen in the 2006 cyber

incident in Alaska and more recent attacks (Austin et al., 2023; CSIS, 2024; Goodin, 2022). Despite technological progress, the increasing reliance on automation and space-based systems has introduced new vulnerabilities (Elmarady & Rahouma, 2021; Sampigethaya et al., 2008). While technical defences have been prioritized in cybersecurity planning, the role of ATCOs has been largely overlooked (AlDaajeh et al., 2022; Nystad et al., 2021). Human-centered strategies remain underdeveloped, even as reports from EUROCONTROL (2021) highlight a 530% rise in aviation cyber-attacks, underscoring the urgency of a more holistic approach to cybersecurity.

Human Factors Engineering (HFE) offers a promising path to enhance cybersecurity by focusing on the interaction between people, systems, and environments. By improving interface design, reducing human error, and aligning cybersecurity strategies with real-world operations, HFE can strengthen system resilience to cyberthreats. This study explores how HFE principles can be more effectively integrated into ATC cybersecurity protocols to safeguard the evolving ATM environment. The following literature review examines the structure and function of ATC systems, emerging cybersecurity threats, and the application of HFE to enhance operational safety and resilience in the digital age.

CYBERSECURITY THREATS IN ATC

Early radar systems revolutionized ATC by enabling aircraft separation and flight tracking. The continued focus on digital modernization has further enhanced ATM system capabilities to keep pace with growing air traffic demand (Tamimi et al., 2020). While the introduction of NextGen technology has improved accuracy and efficiency (Elmarady & Rahouma, 2021), implementing these technologies has introduced significant cybersecurity vulnerabilities (Tamimi et al., 2020). Nextgen initiatives, notably the Controller–Pilot Data Link Communications (CPDLC), Automatic Dependent Surveillance-Broadcast (ADS-B), and Global Navigation Satellite System (GNSS), play an critical role in enhancing the capabilities of ATM system infrastructure to accommodate the increasing air traffic density, it also heightens the system's susceptibility to cyber threats, mainly due to the digital sophistication integrated into CNS systems (Hird, 2021). For example, the shift from voice communication to data link communication (e.g., CPDLC) between ATCOs and pilots raises the risk of intentional manipulation, alteration, or deletion of messages by malicious actors. Furthermore, the widespread adoption of automatic dependent surveillance-broadcast (ADS-B) across numerous ATC facilities aims to enhance real-time precision and accuracy in flight monitoring (Elmarady & Rahouma, 2021). However, the potential for malicious impersonation of an aircraft presents a threat, potentially granting unauthorized access to the system and resulting in undesired outcomes.

Furthermore, the rise of software-defined radios (SDRs) and space-based signals has enabled hackers to conduct cyber-attacks involving false data injection and malware, potentially causing delays, financial losses, or safety threats (Hird, 2021). Recognizing these risks, researchers and

agencies have underscored the urgent need for cybersecurity measures in ATM, including encryption, authentication, firewalls, and audits (AlDaajeh et al., 2022; Atkins & Sampigethaya, 2023; Strohmeier et al., 2017). Still, human-centered cybersecurity protocols that reflect ATCOs' capabilities and limitations remain underdeveloped (Guastello, 2023).

HUMAN FACTORS ENGINEERING (HFE) PRINCIPLES

Human error significantly impacts aviation operations, with approximately 70% of accidents attributed to human factors (Kansoy & Bakanoğlu, 2021), Rooted in psychology, engineering, and design, HFE aims to reduce errors and increase user satisfaction by designing intuitive systems that account for human capabilities and limitations (Boston-Fleischhauer, 2008; Chapanis, 1983; Salvendy, 2012). Understanding HFE principles aids in designing systems that support cognitive functioning and reduce the likelihood of errors (Endsley, 1995). ATC systems integrate HFE into their design (Austrian & Piccione, 2013). For example, high-contrast displays, clear auditory alerts (Lyu et al., 2019), and ergonomic workstations to reduce strain and improve precision (Norman, 2013). Decision-support tools and memory aids help ATCOs manage aircraft, make timely decisions, and retain critical information under pressure (Endsley, 1995; Wickens et al., 2020). Overall, HFE principles support perception, psychomotor coordination, and cognitive processes in the human-machine interaction.

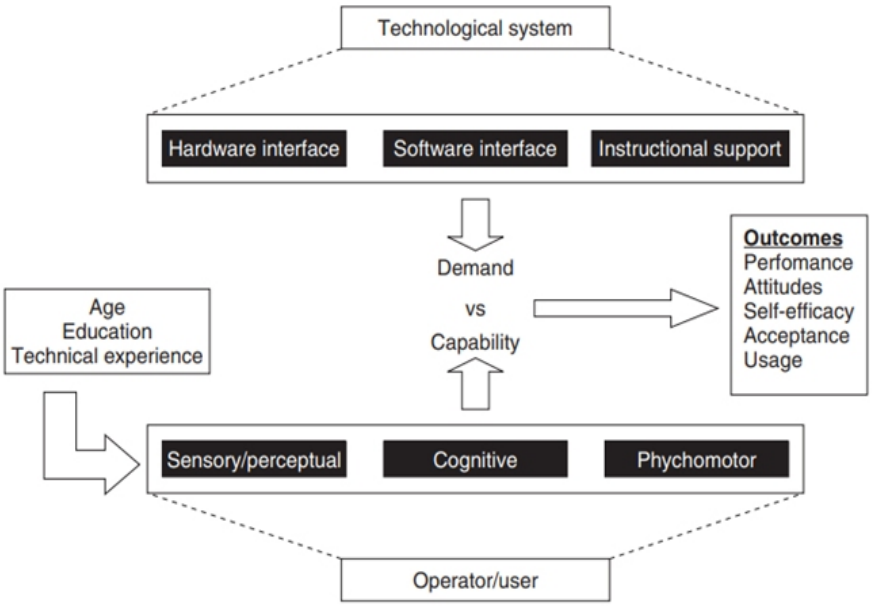

Figure 1: A general model of the human-machine system, adapted from (Guastello, 2023).

TECHNOLOGY NECESSITATES HFE APPLICATION

Besides cybersecurity concerns, the advanced ATC technology have transformed human-machine systems, introducing intelligent machines that augment human capabilities and shifting the human role from direct control to system monitoring (Endsley, 2017; Guastello, 2023). In addition, although automation enhances efficiency and reduces errors, it also increases cognitive demands, heightens risks of automation bias and distrust, and can lead to skill degradation if operators lose manual proficiency or become overly reliant on systems (Casner & Schooler, 2014; Endsley & Kiris, 1995). While acknowledging the technology benefits, the modern human-machine systems should be designed supporting the evolving roles of ATCOs and maintain safety and performance (Austrian & Piccione, 2013; Guastello, 2023).

Integrating HFE into ATC systems provides a user-centered approach to enhancing human-machine systems, therefore result in cybersecurity resilience, operational safety, and efficiency. By aligning system design with human cognitive and physical capabilities, HFE reduces the likelihood of human error (Guastello, 2023; Wickens et al., 2020). Intuitive interfaces, real-time alerts, and automated monitoring systems ease cognitive load and enable faster, more accurate threat detection, while ergonomic workstations and customizable displays improve usability and accommodate diverse controller needs (Endsley, 2017; Kearney et al., 2016; Norman, 2013; Sweller, 2011). HFE also strengthens SA, supports workload and stress management, and enhances training through clear information design, optimized task structures, and simulation-based learning (Dattel et al., 2022; Endsley, 1995). By addressing individual differences and fitting tasks to user abilities, HFE promotes resilient, adaptive ATC environments that are better equipped to respond to evolving cybersecurity threats (Guastello, 2023; Simonson et al., 2023).

METHOD

This study investigates how HFE principles can be applied to address cybersecurity challenges in ATC. Through the use of an exploratory qualitative research approach, the study combines a literature review with an analysis of government documents, case studies, news articles, and industry best practices. Data collection centers on scholarly articles, research papers, and official reports from databases including journals, Google Scholar, and online libraries, guided by keywords related to HFE, ATCOs, and ATC cybersecurity. Only peer-reviewed journal articles from the past 15 years are included to ensure source relevance.

The analysis integrates theoretical, practical, and real-world perspectives to extract key themes and comprehensively understand how HFE can enhance ATC cybersecurity. Literature provides the theoretical base, while government and industry documents offer practical guidelines. Case studies demonstrate applied outcomes and news articles capture current developments and public sentiment. These insights are synthesized into a conceptual framework illustrating the integration of HFE in ATC cybersecurity, identifying best practices and areas for future exploration. This

approach supports the development of intuitive, user-friendly cybersecurity solutions tailored to the complex demands of the ATC environment.

DISCUSSION

Designing systems and workplaces with HFE at the core ensures alignment with human capabilities, limitations, and expectations—an approach particularly crucial in the context of ATC, where safety, performance, and cognitive demands are paramount. HFE principles, as defined by the International Labour Organization (ILO) and the International Ergonomics Association (IEA, 2021), emphasize the enhancement of user experience, reduction of errors, support for individual differences, and alignment of system tasks with human abilities. These principles have been validated through numerous studies and government guidelines in system design (Bernard et al., 2020; Rock et al., 2016) and are deeply embedded in the philosophies guiding ATC system development (Austrian & Piccione, 2013; Brown, 2016; Huber et al., 2022). The HFE principles outlined by ILO have been found to parallel with the human factor's philosophies in ATC. Table 1 compares the HFE principles in ATC cybersecurity.

Table 1: Comparison of HFE principles in ATC cybersecurity.

HFE Principle	Definition	Implications for ATC Cybersecurity Solutions
User-Centered Design	An approach that places the user at the forefront of the design process, ensuring systems are tailored to meet users' needs, abilities, and cognitive processes.	Creating interfaces that reduce cognitive workload enhancing the ability of ATCOs to manage cybersecurity threats effectively.
Reducing Errors	Designing systems to minimize the potential for human error, considering human limitations such as attention, perception, and memory.	Implementing automation and real-time alerts to assist ATCOs in detecting and responding to cyber threats, reducing the likelihood of errors.
Safety First	Prioritizing the prevention of harm to users and others by designing systems, procedures, and environments that emphasize safety.	Developing comprehensive training programs to enhance ATCOs' awareness and preparedness for cyber threats, ensuring overall safety.
Accommodation of Individual Differences	Designing systems that function well for diverse users, accommodating varying physical, cognitive, and sensory abilities.	Customizable interfaces and ergonomic workstations to support ATCOs' varying needs and capabilities, improving performance and reducing cognitive load.

Continued

Table 1: Continued

HFE Principle	Definition	Implications for ATC Cybersecurity Solutions
Fit the Task to the Person	Ensuring that the work demands do not exceed the user's physical and cognitive abilities by designing tasks and systems to match user capabilities.	Optimizing workloads and providing tools to reduce stress and fatigue, ensuring ATCOs can maintain high performance and alertness when handling cybersecurity threats.

THE HUMAN-CENTERED APPROACH IN ATC CYBERSECURITY

As a cornerstone of HFE, user-centered design, recognizes that human variability, such as fatigue, distraction, and error, is a major factor in system performance (Wickens et al., 1997), and aims to ensure that ATC systems align with ATCOs' cognitive abilities and needs, enhancing usability and operational effectiveness (Inoue et al., 2015). ATCOs constantly process large volumes of information, and unexpected cyber threats can increase cognitive demands, potentially affecting performance. Interfaces that match natural human information-processing patterns can reduce cognitive load, helping ATCOs focus on essential tasks (Wickens et al., 2020), as well as supporting anomaly detection, SA, and error reduction (ILO & IEA, 2021; Landry, 2011; Ohneiser et al., 2018). Modern ATM interface designs grounded in HFE principles that incorporate intuitive layouts, consistent visual cues, and minimal distractions to improve usability, help ATCOs remain focused, and enhance decision-making, can be especially supportive when faced with cybersecurity incidents.

In conjunction with design, automation help overcome human limitations (e.g., limited attention, memory lapses, and fatigue; Wickens et al., 2020) to assist ATCOs by managing routine tasks, allowing the operators to focus on complex decision-making (Endsley, 2017). Real-time alerts and machine learning detection aid can improve detection effectiveness and reduce response time in detecting ADS-B spoofing (Atkins & Sampigethaya, 2023; Kearney et al., 2016). However, automation must be implemented thoughtfully. Overreliance in automation or poorly designed systems can lead to problems like false alarms and mistrust in the system, thus impairing performance (Endsley, 2017; Rovira & Parasuraman, 2010). This underscores the necessity of applying HFE principles to guide user-centered, intuitive interface design that minimizes disruptions for human operators (Brown, 2016).

Despite the growing importance of cybersecurity, ATCOs often lack adequate training in this area, leading to gaps in awareness, increased workload, and diminished trust in automated defenses (FAA, 2022; Nystad et al., 2021). Simulation-based, interactive training have been shown to significantly improve recognition of threats, decision-making skills, and performance under stress (Liu et al., 2023; Simonson et al., 2023). Yet current training initiatives such as the FAA's AT-CTI program still fall short in

addressing cybersecurity content (McCauley & Broach, 2019). Incorporating tailored training modules that reflect real-world cyber scenarios will be essential for increasing system resilience and operator competence.

Furthermore, recognizing individual physical, sensory, and cognitive diversity improves system usability, safety, and effectiveness (Wickens et al., 2020). In ATC, this means creating customizable interfaces to support diverse visual and cognitive needs (Guastello, 2023), implementing ergonomic workstations to minimize physical strain and support sustained focus, and administering adaptive training to ensure learning and retention effectiveness (Rohrer & Pashler, 2012). These HFE considerations can not only enhance usability but also reduce fatigue and cognitive load, minimizing the likelihood of performance breakdowns during cyber threat detection (Simonds & Brock, 2014).

In the high demanding context of ATC, excessive workload can impair human attention, memory, decision-making, and reaction time, effects that are particularly detrimental when detecting cybersecurity threats (Sweller, 2011; Zhang et al., 2019). The principle of fitting the task to the person involves aligning work demands with individual capabilities to lower stress, mental demand, and human error. In cybersecurity operations, strategies like ergonomic workspace design, optimized shift scheduling, and workload balancing are critical (Costa, 1995; Endsley, 2017; Sweller, 2011). When systems are designed with the user in mind, individuals are more likely to perform at their best.

RECOMMENDATIONS

In light of the findings presented in this study, it is recommended that future developments in the ATM systems place a strong emphasis on integrating HFE principles. This integration should specifically focus on emphasizing user-centered designs to reduce cognitive load, thereby improving the effectiveness of cybersecurity measures. Additionally, regulatory bodies and ATC organizations should consider establishing more rigorous training programs tailored to enhance ATCOs' awareness and responsiveness to cybersecurity threats. Such training programs should incorporate simulations and real-time feedback to improve skill acquisition and decision-making in the face of potential cyber-attacks. This training is further imperative to foster a culture of continuous improvement and adaptive learning within ATC environments to keep pace with the rapid advancements in technology and the evolving nature of cyber threats.

The alignment between theoretical insights and practical strategies underscores the importance of a human-centered approach in designing resilient and efficient ATC systems. HFE are interconnected; neglecting any single principle undermines the overall effectiveness. Solely considering one principle while overlooking another will prove ineffective. Therefore, integrating all identified HFE principles from the literature into ATC cybersecurity solutions offers a comprehensive approach to improving system resilience and safety. These protocols not only support ATCOs in their critical roles but also ensure the overall safety and efficiency of the ATM system.

CONCLUSION

Advancements in modern technology have significantly enhanced the capabilities of the ATM system. However, protecting the system from cybersecurity challenges remains a complex issue that has yet to be fully addressed. By emphasizing the human element, this study challenges the traditional focus on purely technical solutions and underscores the critical role of HFE in cybersecurity solutions.

Theoretically, the research expands the body of knowledge by demonstrating that effective cybersecurity solutions must be user-centered, reducing cognitive workload and minimizing the potential for human error. It establishes a robust framework for understanding how HFE principles can be strategically applied to create more intuitive, efficient, and safer ATC systems. This holistic approach not only improves system performance but also ensures that the solutions are tailored to meet the diverse needs and capabilities of ATCOs.

Practically, the study offers tangible benefits for enhancing ATC cybersecurity. Integrating HFE principles into cybersecurity measures can lead to the development of more effective and user-friendly protocols, thereby increasing the overall resilience of ATC systems to cyber threats. By providing insights into the practical application of HFE in ATC cybersecurity, the research suggests the human-centered approach in future designs of the ATM system. These practical recommendations are aimed at enhancing the preparedness and responsiveness of ATCOs to cyber threats, ultimately safeguarding the integrity and efficiency of the aviation ecosystem.

REFERENCES

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*. https://doi.org/10.1016/j.cose.2022.102754

Atkins, G., & Sampigethaya, K. (2023). Air traffic control system cyber security using humans and machine learning. *2023 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, 1–14. https://doi.org/10.1109/ICNS58246.2023.10124305

Austin, K., Mackintosh, T., & Harrison, E. (2023, August). *Cancelled flights: Air traffic disruption caused by flight data issue*. BBC News. https://www.bbc.com/news/uk-66644369

Austrain, E., & Piccione, D. (2013). The FAA's human factors air traffic control / technical operations strategic research plan. *17th International Symposium on Aviation Psychology, 50–55*. https://corescholar.libraries.wright.edu/isap_2013/102

Bernard, F., Zare, M., Sagot, J.-C., & Paquin, R. (2020). Using digital and physical simulation to focus on human factors and ergonomics in aviation maintainability. *Human Factors, 62*(1), 37–54. https://doi.org/10.1177/0018720819861496

Boston-Fleischhauer, C. (2008). Enhancing healthcare process design with human factors engineering and reliability science, part 1: Setting the context. *The Journal of Nursing Administration, 38*(1), 27–32. https://doi.org/10.1097/01. NNA.0000295632.80345.3d

Brown, J. P. (2016). The effect of automation on human factors in aviation. *Journal of Instrumentation, Automation and Systems, 3*(2). https://doi.org/10.21535/jias.v3i2.916

Casner, S. M., & Schooler, J. W. (2014). Thoughts in flight: Automation use and pilots' task-related and task-unrelated thought. *Human Factors, 56*(3), 433–442. https://doi.org/10.1177/0018720813501550

Chapanis, A. (1983). *Introduction to human factors considerations in system design*. NASA, Goddard Space Flight Center Human Factors Considerations in System Design.

Costa, G. (1995). Occupational stress and stress prevention in air traffic. International Labour Office. Working paper: CONDI/T/WP, 6.

Dattel, A. R., Goodwin, T., Brodeen, H., Friedenzohn, D., Ochoa, O., Wang, H., Gao, P., Haris, S., Parkar, I. (2022). Using virtual reality for training to identify cyber threats in the bridge of a ship. *Proceedings of the Human Factors and Ergonomics Society 66th Annual Meeting*.

Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE Access, 9*. https://doi.org/10.1109/ACCESS.2021.3121230

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Endsley, M. R. (2017). From here to autonomy: Lessons learned from human–automation research. *Human Factors, 59*(1), 5 27. https://doi.org/10.1177/0018720816681350

Endsley, M. R., & Kiris, E. O. (1995). The out-of-the-loop performance problem and level of control in automation. *Human Factors, 37*(2), 381-394. https://doi.org/10.1518/001872095779064555

EUROCONTROL. (2021, June). *Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?* https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime

Federal Aviation Administration. (2022). *Budget estimates fiscal year 2023*. U. S. Department of Transportation. https://www.transportation.gov/sites/dot.gov/files/2022-03/FAA_Buget_Estimates_FY23.pdf

Hird, J. (2021). Air traffic management: A cybersecurity challenge. EUROCONTROL. https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf

Inoue, S., Yamazaki, K., Hirako, H., & Sasaki, T. (2015). Applying human centered design process for designing air traffic control interfaces. *International Conference of Design, User Experience, and Usability*, 307–316. https://doi.org/10.1007/978-3-319-20898-5_30

Goodin, D. (2022, October). *GPS interference caused the FAA to reroute Texas air traffic. Experts stumped*. Ars Technica. https://arstechnica.com/information-technology/2022/10/cause-is-unknown-for-mysterious-gps-outage-that-rerouted-texas-air-traffic/

Guastello, S. J. (2023). *Human factors engineering and ergonomics: A systems approach*. CRC Press.

Huber, S., Gramlich, J., Pauli, S., Mundschenk, S., Haugg, E., & Grundgeiger T. (2022). Toward user experience in ATC: Exploring novel interface concepts for air traffic control. *Interacting with Computers, 34*(2), 43–59. https://doi.org/10.1093/iwc/iwac032

International Labour Office, & International Ergonomics Association. (2021). *Principles and guidelines for human factors/ergonomics (HFE) design and management of work systems*. https://www.ilo.org/publications/principles-and-guidelines-human-factors-ergonomics-hfe-design-and

Kansoy, S. U. & Bakanoğlu, K. (2021). The importance of human factors in aviation companies. *International Journal of Arts and Social Science, 4*(2). https://www.ijassjournal.com/2021/V4I2/4146575549.pdf

Kearney, P., Li, W.-C., & Lin, J. J. H. (2016). The impact of alerting design on air traffic controllers' response to conflict detection and resolution. International *Journal of Industrial Ergonomics, 56*, 51–58. https://doi.org/10.1016/j.ergon.2016.09.002

Kroemer, K. H. E., & Kroemer, K. H. E. (2009). Fitting the human: Introduction to ergonomics (6th ed.). CRC Press.

Liu, D., McSorley, J., Blickensderfer, E., Vincenzi, D. A., & Macchiarella, N. D. (2023). Transfer of training. In D. A. Vincenzi, M. Moloua, P. A. Hancock, J. A. Pharmer, & J. C. Ferraro, (Eds.). *Human Factors in Simulation and Training*. Taylor & Francis Group.

Lyu, T., Song, W., & Du, K. (2019). Human factors analysis of air traffic safety based on HFACS-BN model. *Applied Sciences, 9*(23). https://doi.org/10.3390/app9235049

McCauley, D., & Broach, D. (2019). A history of the air traffic control collegiate training initiative (AT-CTI) program. *20th International Symposium on Aviation Psychology,* 444–449. https://corescholar.libraries.wright.edu/isap_2019/75

Norman, D. A. (2013). *The design of everyday things*. Basic Books.

Nystad, E., Simensen, J. E., & Raspotnig, C. (2021). Investigating operative cybersecurity awareness in air traffic control. *2021 14th International Conference on Security of Information and Networks (SIN), 1*, 1–8. https://doi.org/10.1109/SIN54109.2021.9699158

Ohneiser, O., Jauer, M., Rein, J., & Wallace, M. (2018). Faster command input using the multimodal controller working position "tricontrol." *Aerospace, 5*(2), 54. https://doi.org/10.3390/aerospace5020054

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man and Cybernetics. Part A, Systems and Humans, 30*(3), 286–297. https://doi.org/10.1109/3468.844354

Pereira, B. A., Lohmann, G., & Houghton, L. (2022). Technology trajectory in aviation: Innovations leading to value creation (2000-2019). *International Journal of Innovation Studies,* 6(3), 128–141. https://doi.org/10.1016/j.ijis.2022.05.001

Rock, C., Cosgrove, S. E., Keller, S. C., Enos-Graves, H., Andonian, J., Maragakis, L. L., Gurses, A. P., & Xie, A. (2016). Using a human factors engineering approach to improve patient room cleaning and disinfection. *Infection Control and Hospital Epidemiology, 37*(12), 1502–1506. https://doi.org/10.1017/ice.2016.219

Rohrer, D., & Pashler, H. (2012). Learning styles: Where's the evidence? *Medical Education*, *46*(7), 634–635. https://doi.org/10.1111/j.1365–2923.2012.04273.x

Rovira, E., & Parasuraman, R. (2010). Transitioning to future air traffic management: Effects of imperfect automation on controller attention and performance. *Human Factors, 52*(3), 411–425. https://doi.org/10.1177/0018720810375692

Salvendy, G. (Ed.). (2012). *Handbook of human factors and ergonomics*. John Wiley & Sons.

Sampigethaya, K., Poovendran, R., & Bushnell, L. (2008). Secure operation, control, and maintenance of future e-enabled airplanes. *Proceedings of the IEEE, 96*(12), 1992–2007. https://doi.org/10.1109/JPROC.2008.2006123

Simonds, T. A., & Brock, B. L. (2014). Relationship between age, experience, and student preference for types of learning activities in online courses. *Journal of Educators Online, 11*(1). https://doi.org/10.9743/JEO.2014.1.3

Simonson, R. J., Williams, K. N., Keebler, J. R., & Lazzara, E. H. (2023). Simulation-based training for decision-making. In D. A. Vincenzi, M. Moloua, P. A. Hancock, J. A. Pharmer, & J. C. Ferraro, (Eds.). *Human Factors in Simulation and Training*. Taylor & Francis Group.

Strohmeier, M., Schafer, M., Pinheiro, R., Lenders, V., & Martinovic, I. (2017). On Perception and reality in wireless air traffic communication security. *IEEE Transactions on Intelligent Transportation Systems, 18*(6), 1338–1357. https://doi.org/10.1109/TITS.2016.2612584

Sweller, J. (2011). Cognitive load theory. In *Psychology of Learning and Motivation*, *55*, 37–76. Academic Press.

Tamimi, A., Hahn, A., & Roy, S. (2020). Cyber threat impact analysis to air traffic flows through dynamic queue networks. *ACM Transactions on Cyber-Physical Systems, 4*(3), 1–22. https://doi.org/10.1145/3377425

Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2020). *Engineering psychology and human performance*. Routledge.

Wickens, C. D., Mavor, A. S., & McGee, J. P. (1997). *Flight to the future: Human factors in air traffic control*. National Academy Press.

Zhang, X., Yuan, L., Zhao, M., & Bai, P. (2019). Effect of fatigue and stress on air traffic control performance. *2019 5th International Conference on Transportation Information and Safety (ICTIS)*, 977–983. https://doi.org/10.1109/ICTIS.2019.8883823