Human Factors in Cybersecurity, Vol. 53, 2022, 74–83
https://doi.org/10.54941/ahfe1002204

Assessing Human Factors and Cyber Attacks at the Human-Machine Interface: Threats to Safety and Pilot and Controller Performance

Mark Miller and Sam Holley

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

ABSTRACT

The current state of automated digital information in aviation continues to expand rapidly as NextGen ADS-B(In) systems become more common in the form of Electronic Flight Bag (EFB) pad devices brought onto the flight deck. Integrated systems including satellites, aircraft, and air traffic control (ATC) data currently are not effectively encrypted and invite exposure to cyber attacks targeting flight decks and ATC facilities. The NextGen ATC system was not designed from the outset to identify and nullify cyber threats or attempts at disruption, and the safety gap has enlarged. Performance error at digital human-machine interfaces (HMI) has been well documented in aviation and now presents a potentially significant threat where the HMI can be more susceptible to human error from cyber attacks. Examples of HMI errors arising from digital information produced by automated systems are evaluated by the authors using HMI flaws discovered in recent Boeing 737-Max accidents. SHELL computer diagrams for both the digital flight deck and ATC facilities illustrate how the system is now interconnected for potential cyber threats and identifies how human factors consequences compromising HMI safety and operator performance present potential dangers. Aviation Safety and Reporting System (ASRS) data are examined and confirm HMI threats. The authors contrast various HMI errors with cyber attack effects on cognition, situational awareness, and decision making. A focused examination to assess cyber attack effects on cognitive metrics suggests cognitive clarity of operators is confounded when confronted with conflicting or confusing indications at the HMI. Difficulty in successfully identifying a cyber attack and the actions taken as human factors countermeasures are illustrated in the context of the HMI environment. The Human Factors Analysis and Classification System (HFACS) is used to show how cyber attacks could occur and be addressed along with a dual-path solution.

Keywords: NextGen, Cyber attack, SHELL, HMI, Cognitive load, HFACS

THE DIGITAL AGE OF NEXTGEN FLIGHT AND ENABLING TECHNOLOGIES

Computer information and automation in the United States National Airspace System (NAS) is rapidly enhancing safe and efficient flight operations through cockpit and ATC technologies. The digital age is solidly established in the NAS through a network of technologies and satellites known as the

NextGen Air Transportation System (NextGen). The ATC approach traffic controller (TRACON) can manage more aircraft through Standard Terminal Automation Replacement System (STARS) control displays by using enhanced communications augmented with multiple information links. Ground-based ATC infrastructure is being replaced with digital satellite data. The digital data connects a new era of pilots to the ATC system with ADS-B(Out) devices that upgrade the transponders in aircraft. The enhanced digital system brings to the flight deck updated flight safety information through ADS-B(In) which is also integrated into the EFB for pilots. Pilots benefit when flying with ADS-B(In) through added situational awareness of other aircraft, terrain, and weather, all displayed live from the EFB which is uploaded prior to boarding (Bertorelli, 2022).

THE NEED FOR ENHANCED CYBER AWARENESS ALONG THE DIGITAL HMI

Proliferation of ADS-B(In) technologies in portable pilot EFBs along with other NextGen technologies mark the age of digital flight in the NAS and open a real threat of increasing cyber attacks against aircraft and ATC facilities. The increased use of digital technologies and growing aircraft density (including unmanned aerial systems) and interoperability with satellites invite potential targets for cyber attacks. Few of these systems were developed with embedded cyber security in their designs which reveals a potential increase in exposure for cyber attacks. In terms of aviation safety and risk management, the severity of the cyber threat also needs to be considered. Consequently, the question arises as to whether a cyber attack in the NAS could cause a catastrophic commercial aviation accident mediated through aircraft equipment, ATC TRACON or the satellite system. The authors contend that at this juncture a direct cyber attack causing a catastrophic accident would, by itself, be highly unlikely in the NAS which maintains current cyber risks at acceptable levels. Supporting an elevated safety severity assessment for cyber attacks is that future attacks are more likely to occur along the digital HMI and thus the human operator will be involved in the attack and challenged to adopt and overcome the consequences. For a cyber attack to be catastrophic, the human operator in the digital HMI would have to fail due to human error. In modern aviation safety and human factors, 80% of commercial aviation accidents in the U. S. are caused by human error (Rankin, 2007). A cyber attack with planned intent to use aviation digital technology as the portal or agent will engage a human operator. How the end user overcomes a cyber attack along the digital HMI to maintain safe flight is where the element of human error could manifest, hence the need for human factors solutions.

Cyber Attack and Human Error on the Digital HMI

To demonstrate how a cyber attack could trigger a chain of human error events along the digital HMI to cause an accident, examples of the Boeing 737 Max 8 crashes of Indonesia and Ethiopia are applicable. In the catastrophic accidents of Lion Air Flight 610 in October 2018 and Ethiopian

Airlines Flight 302 five months later, the central causal factor was the automated Maneuvering Characteristics Augmentation System (MCAS) (NTSB, 2019). In both cases a faulty angle of attack vane input sensor, one of two on board, triggered the automated MCAS system to push the nose of the aircraft down and in both cases the pilots were unable to correct MCAS. Modifying an older 737 model and adding more powerful engines meant that the new 737 Max 8 aircraft would result in the nose of the aircraft moving upward as power was applied potentially leading to a dangerous aerodynamic stall. The MCAS system acquires signals from two angle of attack vanes (right and left) and if one of the signals alerts the MCAS of an eminent stall, the MCAS system automatically compensates and forces the nose of the aircraft down to prevent the stall. In both cases the NTSB brought forth the fact that the pilots became cognitively overwhelmed and confused by the wide array of alarms and alerts in the cockpit. The NTSB also cited the failure of Boeing to properly assess the potential MCAS sensor problem during the Max 8 certification process with the FAA. Not accounting for the reactions of the pilots to the sensor failure in the certification process resulted in a flawed design of the MCAS system. Weak training on the MCAS system for normal usage and emergency scenarios also contributed a major role in both accidents. Human error related to the digital HMI led to both accidents and invites the possibility that a similar condition could be produced if a purposeful cyber attack occurred with a system like MCAS.

Cyber Analysis of the NextGen System in Aircraft and ATC

The diagram (Figure 1) shows places that would invite cyber attacks in the NextGen system via digital technologies in aircraft, ATC, ADS-B ground stations, and GPS and communications satellites. These threat areas should be a priority for cyber security to prevent attacks. The diagram also presents a clear portrayal of how digital flight is operating in the NAS and NextGen system. Digital positional data is linked from GPS satellites to the aircraft and ATC along with ADS-B ground stations. ADS-B(In) data are also being relayed along the same digital links. Meanwhile digital communications from ATC to the aircraft are linked via communications satellites. The unique aspect of this diagram is that it illustrates how all the principal components are now inter-connected digitally. A cyber breach could occur anywhere in this system to influence aircraft and ATC.

Cyber Attack in Flight/ATC and Digital HMI SHELL Analysis

Cyber security is an effective prevention tool, but when cyber attacks do occur they are likely to affect the digital HMI. Challenges to operators working along the digital HMI are represented in Figure 1 which illustrates the potential for human error from a cyber attack in aircraft and ATC. For aircraft, compromised GPS data could affect the navigation system or the ADS-B(In) data presented on the pilots' EFB. The digital texting used for Datalink could also provide opportunity for a potential human error. The updated SHELL model (Miller, 2017) shows the interaction of computer informational and automation devices in the modern cockpit and how the

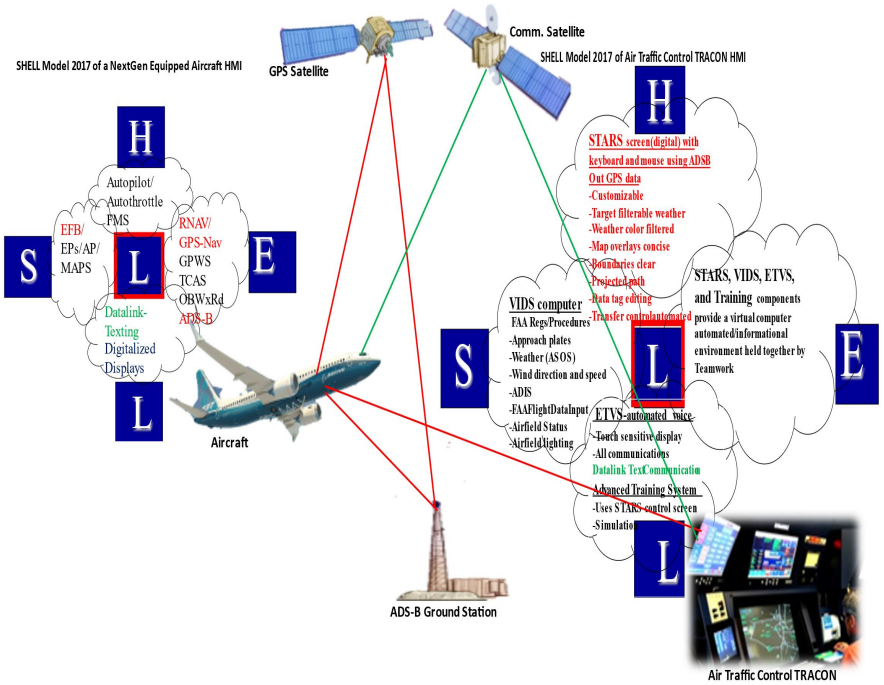

Figure 1: The NextGen air transportation system with digital HMI.

once direct linkages in the HMI interfaces now have digital HMI overlapping clouds to work through as interface linkages. The digital clouds in the case of aircraft HMI highlight concern about a cyber attack in that the new digital HMI is already cluttered with overlapping digital technologies that can lead to excessive cognitive workload and exacerbate distractions that degrade cognitive processing. Introducing a cyber attack, and the attendant distraction or confusion affecting pilots already challenged by overlapping digital HMI, could lead to human error. In the case of the ATC TRACON, a potential cyber attack to the system could directly affect controllers through the STARS display computer which has digital information and automation tools to control aircraft accurately and efficiently. The SHELL Model (Miller et al. 2019) for the TRACON controller in Figure 1 shows the operator in relation to the digital HMI cloud interfaces. Distraction caused by a cyber attack to the STARS computer display or to digital communications, either recognized as a cyber attack or not, would challenge controllers cognitively during control of aircraft and could result in human error.

HUMAN FACTORS FOR REDUCING CONSEQUENCES ALONG THE HMI

Figure 1 pointedly shows that aviation in its rapidly expanding digital future is no longer just a potential cyber security problem to be resolved by stalwart preventative measures. Instead, the cyber threat to aviation will be a challenge by managing human error along the digital HMI and reducing the consequences of attacks when they do occur. Juxtaposed to the preventative side of

aviation safety is the fact that human error in relation to accident or incident causal event chains (Hawkins, 1987) can still occur and reducing the consequences of cyber attacks will call for human factors digital HMI strategies to complement cyber prevention strategies. To that end, should cyber attacks occur in flight or in ATC the question arises as to whether pilots and controllers will be able to overcome the issues in the digital HMI or, conversely, whether the attack will trigger a series of human errors. Reducing the consequences of the cyber attack should be accomplished through human factors counter measures. Adopting an approach used by U.S. Naval Aviation provides an effective example where pilots employ human factors to overcome a cyber attack on the digital HMI in the cockpit by applying Crew Resource Management (CRM) with Threat Error Management (TEM). Through CRM training pilots can use the benefits of TEM incorporated with the CRM to prepare and become more aware of how a cyber attack manifests, while also using TEM to immediately recover from any undesirable state caused by a cyber attack (U.S. Navy, 2004). When considering ATC TRACON and reducing the consequences of cyber attack, a demonstrated solution could come in the form of resiliency engineering as used by Euro Control applying a form of scenario-based training that helps with degraded ATC sectors during events such as a cyber attack (Jaksic & Janic, 2020). This would mean that the ATC TRACON sector might be considered resilient if the systems could be restored close to a nominal level by employing effective contingency measures. Contingency measures could include using "manual mode", changing control arrangements, or using backup equipment. The objective is to continually train to 'what if' scenarios to achieve an acceptable level of resiliency engineering.

ASRS Data Supporting a Cyber Human Factors Model for Aviation

A cyber attack on the digital HMI calls for cyber human factors counter measures substantially supported by data from recent NASA ASRS voluntary incident reports. The ASRS data selected by the authors were related to the U.S. commercial aviation industry and the NextGen system and included three separate data sets for different reporting categories: GPS reports, Passenger Electronic Device reports and ATC reports. All three categories were chosen for their direct relation to potential interference regarding the digital HMI. The GPS reports represent the digital technology used in the NextGen system for ATC to track aircraft through satellites while supported by ADS-B. The GPS data set included the 50 most recent voluntary reports from airline pilots during the periods from July-December 2018. Of the 50 reports, nine (18%) indicated problems related to navigation, instrument approaches and RNAV technology caused by GPS malfunctions, and all were related to flight deck digital HMI. The Passenger Electronic Device reports show how electronic devices can have a direct effect on the digital HMI in the cockpit. Although the data of the 50 most recent reports spanned a lengthy period from November 2006-November 2018, there were eight (16%) that were directly related to passenger devices electronically affecting the electronic navigation and communications equipment of commercial airplane

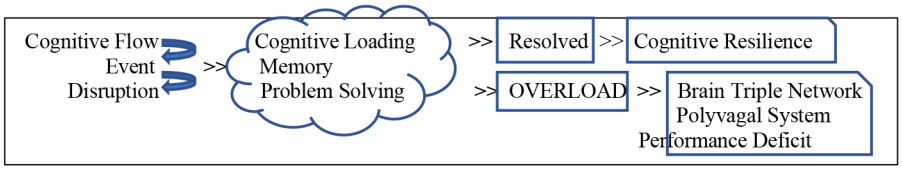

Figure 2: Effects on cognitive processing from cyber attack at HMI.

cockpits (ASRS, 2018). The ATC reports were reported during a time span of two months from January-February 2019. Of the 50 voluntary reports over the relatively short time span, three (6%) were related to issues in the digital HMI of the TRACON ATC (ASRS, 2019). All three data sets indicate notable percentages of incidents reported by pilots and ATC along the digital HMI that show potential vulnerability to cyber-attacks in the NextGen system and the potential for human error. The authors conclude these reports represent scenarios that potentially could be generated through cyber attacks and are remiss of 5G issues. Consequently, the need for human factors awareness and training becomes paramount due to the critical nature of cognitive flow, load, and processing in relation to users of the digital HMI.

Cognitive Flow, Load, and Processing After a Cyber Attack

As exemplified in earlier sections, the consequences of a cyber attack and the effects on cognitive load and processing can present heretofore unforeseen complications. The relationship and interactions of cognitive flow (optimal cognitive performance at near peak capacity), cognitive loading (allocation by priority to available neural resources), and loss of cognitive resilience become of paramount importance with the advent of cyber attack. Disruptions in cognitive flow and processing brought on by alerts, indications of system failure, conflicting information, and similar confounding circumstances occur with recognized threats. The addition of disruption caused by cyber attacks, which may manifest in similar or unfamiliar aspects, expands the scope of cognitive load and the attendant depletion of neural resources as shown in Figure 2. Already approaching maximum processing capability and then tipping into overload when presented with novel or unanticipated situations can result in confusion, delay, and error (from action or inaction). The default mode deficits described in the Triple Brain Model (Menon, 2010) would be realized as well as a compromised parasympathetic nervous system (Porges, 2011) that reduces present-mindedness. It is noteworthy that cognitive metrics are less well understood in these instances. For example, when tasks are performed sequentially or in stages, there typically are adequate resources to accomplish relative successes. When fully enveloped or faced with deconfliction decisions or expanding task complexity the result is cognitive freezing or substantial delay (Giesbrecht et al 2014).

Closer consideration of how events can present as cyber attacks offers enlightened insights into the threats to cognitive load and processing. For flight deck operations, the Cockpit Display of Traffic Information (CDTI) provides a pilot with increased situational awareness of surrounding air traffic when

visual separation is not possible when conducting a CDTI-Assisted Visual Approach that provides ATC and pilots enhanced operational flexibility. In this procedure, separation responsibility shifts from ATC to the flight crew (Bone & Mendolia, 2018). Visual scanning and effective interpretation of symbols are perceptual functions to execute the procedure safely, although these are performed in a dynamic environment that taxes cognitive bandwidth. Cognitive style is an issue that relates how a pilot recognizes, perceives, and processes information and how that influences actions (Kirschner et al. 2018). Where such approaches do not include awareness and strategies for cyber attack effects, the consequences reside in the cognitive cloud overlaying the elements that comprise cognitive loading and are not integrated into the pilot's constructive memory processes. Single pilot operations present a particular issue that compounds the danger since only one operator is available to process the information. Likewise, with distributed crewing (one pilot airborne and another ground-based) (Stanton, 2014) the communication links and coordination required are expanded exponentially. In these instances, the concept of cognitive coupling between humans and machines (Hollan et al. 2000), especially sensitive at the human-machine interface, will likely encounter the uncertainty, delay, and confusion that accompanies cyber attacks.

Importance of Human Factors in a NextGen Cyber Attack

The sequence of a cyber attack along the HMI interface in a commercial aircraft or ATC TRACON is illustrated in Figure 3 via the dotted line on the left side. The human error will start through ineffective Organizational Influences, especially a weak cyber security culture. From there, Unsafe Supervision is affected adversely by the Organizational Influences which can contribute to human error by allowing ineffective cyber security measures. The next level, Preconditions for Unsafe Acts, eventually gives way to a cyber attack in the technological environments of the cockpit or ATC TRACON. Unfortunately, a cyber attack could quickly turn into many forms of potential Unsafe Acts (human errors) in both the cockpit or the ATC digital HMI. These errors are manifested at the bottom of Figure 3 in the form of decision errors, skill-based errors, and perceptual errors.

More troubling is that such attacks could cause significant confusion for the pilot crew or controller where they could commit a routine or purposeful unsafe act to resolve the problem in desperation. To counter a threat such as a cyber attack in aviation, cyber human factors counter measures need to be strategically implemented into the organization from the top as annotated on the right side of the HFACS diagram. From this perspective the leadership of the organization commits the resources to assure preventative cyber security measures and the training resources to resolve effects from cyber attacks if they occur. The leadership of the organization would be expected to endorse an aviation cyber counter measures plan and integrate those measures into the organization flight or ATC strategies. Supervisory management could then move forward with that plan and execute accordingly using cyber security preventative measures while simultaneously preparing pilot and ATC

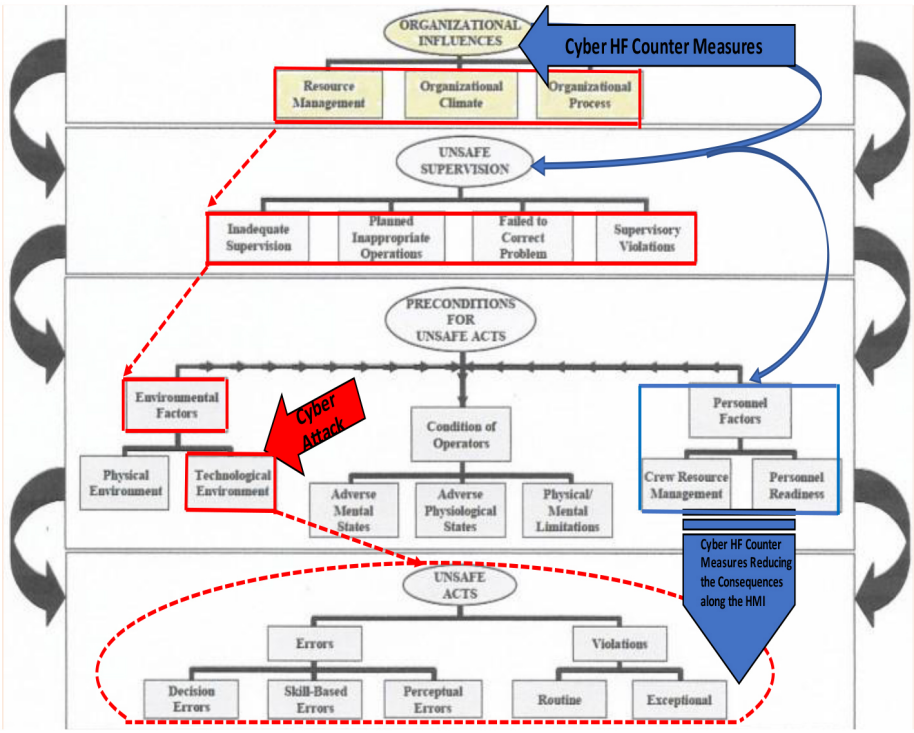

Figure 3: HFACS with potential cyber-attack and HF counter measures. Adapted from Weigmann et al. 2005.

personnel to recognize and respond effectively with a cyber attack should it occur. That training and preparation is depicted in Figure 3 at the Preconditions for Unsafe Acts level where, for example, effective responses could be achieved from CRM training modified to include TEM for pilots or resiliency training for ATC. With appropriate training the cyber situationally aware pilots and ATC can overcome the disruptive effects from cyber attack and be less susceptible to human error.

The cyber attack threat within U.S. airspace is growing. The cyber threat to flight cannot be mitigated with cyber security measures alone, but will require different human factors cyber digital HMI strategies to correct for an attack and reduce human error once it does occur on the flight deck or in the ATC TRACON. Our analysis of air safety voluntary report data from the ASRS system supports that the digital HMI on both the commercial flight deck and the ATC TRACON could be vulnerable to such cyber attacks. Understanding that the nature of such attacks has a serious potential for human error due to the digital HMI and the disruptive interruption of the operator's cognitive flow, load and processing is paramount to designing and training operator human factors cyber mitigation strategies in the future. Cyber attacks in NextGen flight may be thwarted from both preventative cyber security measures and human factors counter measures strategies that will need to be supported from the highest levels of the organization and supervisory management to build a cyber situationally aware and proactive flight or ATC organization.

REFERENCES

ASRS 2019, ASRS Database Report Set, Passenger Electronic Devices, Update 30.0, National Aeronautics and Space Administration, viewed 18 January 2022, <https://asrs.arc.nasa.gov/search/reportsets.html>

ASRS 2018, ASRS Database Report Set, Air Traffic Control Reports, Update 32.0, National Aeronautics and Space Administration, viewed 18 January 2022, <https://asrs.arc.nasa.gov/search/reportsets.html>

ASRS 2018, ASRS Database Report Set, Global Positioning System (GPS), Update 31.0, National Aeronautics and Space Administration, viewed 18 January 2022, <https://asrs.arc.nasa.gov/search/reportsets.html>

Bertorelli, P. 2022, "New ADS-B Portables: Price for Every Purpose: New Products from ForeFlight, Dynon and Appareo", *The Aviation Consumer,*[Online]. vol. 48, no. 12, p. 4.

Bone, R. & Mendolia, A. 2018, "Air traffic controller conduct of a no-closer-than spacing operation", *IEEE Integrated Communications, Navigation, Surveillance Conference (ICNS, pp. 3G3-1-3G3-15*.

Giesbrech, B., Sy, J., Bundesen, C. & Kyllingsbaek, S. 2014, "A new perspective on the perceptual selectivity of attention under load", *Annals of the New York Academy of Sciences*, vol. 1316, no. 1, pp. 71–86.

Hawkins, F.H. 1987, "Human factors in flight", 2nd ed. Aldershot, U.K.: Ashgate

Hollan, J., Hutchins, E. & Kirsh, D. 2000, "Distributed cognition: Toward a new foundation for human-computer interaction research", *ACM Transactions on Computer-Human Interaction*, vol. 7. no. 2, pp. 174–196.

Jaksic, Z. & Janic, M. 2020. "Modeling resilience of the ATC (air traffic control) sectors", *Journal of Air Transport Management*, vol. 89, no. 101891, pp. 1–10.

Kirschner, P. A., Sweller, J., Kirschner, F. & Zambrano R., J. 2018, " From cognitive load theory to collaborative cognitive load theory", *International Journal of Computer-Supported Collaborative Learning*, vol. 13, no. 2, pp. 213–233.

Miller, M. 2017, "Aviation human factors: the SHELL model 2017 and computer/human factors analysis" paper presented at the FAA Aviation Safety Conference, Honolulu, 23 June.

Miller, M., Holley, S., Mrusek, B, & Weiland, L. 2019, "Change in the dark room: Effects of human factors and cognitive loading issues for NextGen TRACON air traffic controllers." In: H. Ayaz (ed.). *Advances in Neuroergonomics and Cognitive Engineering*, vol. 953, Springer, pp. 155–166.

Menon, V. 2010, "Large-scale brain networks and psychopathology: A unifying triple network model", *Trends in Cognitive Science*, vol. 15, no. 10, pp. 483–506.

National Transportation Safety Board, 2019, "Assumptions used in the safety assessment process and the effects of multiple alerts and indications on pilot performance, safety recommendation report", *NTSB-ASR-19-01*, 2019, pp. 1–13.

Porges, S. 2011, The polyvagal theory: Neurophysiological foundations of emotions, attachment, communication, and self-regulation. New York: Norton.

Rankin, W. 2007, "MEDA investigation process", In *Boeing.com/commercial/aeromagazine*, Aero Q207 article 3, pp. 15–21.

Stanton, N. A. 2014, "Representing distributed cognition in complex systems: How a submarine returns to periscope depth", *Ergonomics*, vol. 57, no. 3, pp. 403–418.

U.S. Navy 2004, "CRM 6th Generation briefing on threat and error management", PowerPoint presentation C-050-1503A PPT 5001 01, viewed 25 January 2022, <https://www.coursehero.com/file/82613684/ppttemmodelpptx/>

Wiegmann, D., Faaborg, T., Boquet, A., Detwiler, C., Holcomb, K., Shappell, S. 2005, "Human error and general aviation accidents: A comprehensive, fine-grained analysis using HFACS", Final Report DOT/FAA/AM-05/24, pp. 1–19, Federal Aviation Administration.