FUNCTIONAL COMPLEXITY FAILURES AND AUTOMATION SURPRISES: THE MYSTERIOUS CASE OF CONTROLLED FLIGHT INTO STALL (CFIS)

Lance Sherry,
Center for Air Transportation Systems Research at George Mason University
Fairfax, Virginia
Robert Mauro
Decision Research & University of Oregon
Eugene, Oregon

Nineteen modern airliner Loss of Control (LOC) accidents resulting in aerodynamic stalls were analyzed. These accidents involved structurally and mechanically sound aircraft decelerating through the $1.3V_{Stall}$ buffer to the stall airspeed - i.e. a Controlled Flight into Stall (CFIS). The analysis produced three main observations: First, the accidents were "functional complexity" failures -- the result of a complex sequence of behaviors of the automation functions. There were no consistent: failures that triggered the events (e.g. sensor failures), effects of triggering events on the automation (e.g. mode change), or commands issued by the automation (e.g. thrust setting). Second, the pilots were unable to intervene effectively due to the absence on the flight deck of relevant information and salient cues to monitor these rare events or their effects. Third, there was no single intervention that could mitigate all of these accidents. Implications for flight deck procedures, training and automation design are discussed.

Modern commercial aviation has achieved a remarkable safety record. The 10^{-13} accident rate for modern airliners (IATA, 2013) is four orders of magnitude smaller than the regulatory 10^{-9} target level of safety (ICAO, 2013). This is a testament to the operators, designers and regulators of this transportation system. The low accident rate is a product of the meticulous aviation "safety system" that is the envy of other domains (Bayuk, 2008).

As aviation safety has improved, the character of aviation accidents has changed. Today, commercial aviation accidents are unlikely to be the direct result of a major engine or other equipment malfunction. Instead, they are likely to be the result of a complex combination of technological, environmental, and human factors. In many cases, the accident aircraft itself is mechanically and structurally sound when the accident occurs. This paper describes an analysis of 19 loss of control (LOC) accidents which culminated in an aerodynamic stall. The sequences of events that led to these accidents were examined in an attempt to understand the complex interplay between the factors that precipitated the accidents, rather than determine *the* failure that may have caused each accident.

Methods

Official accident reports and industry airline safety data-bases (e.g. Aviation Safety Network) were searched to identify airline operations (Part 121) and air taxi operations (Part 135) in which aircraft transitioned from safe energy-states within the safe operating speed envelope to an energy-state outside of the safe operating speed envelope by decelerating through $1.3V_{Stall}$ and V_{Stall}. Accidents in the takeoff phase in which the aircraft did not accelerate enough to achieve a safe lift generating airspeed were not considered because a safe flying speed was never achieved. The accident scenarios were identified directly from the accident reports.

Results & Discussion

Nineteen accidents were reviewed. A list and summary of the accidents and their characteristics is included in Sherry et al (2014). All 19 accidents and incidents can be described by the sequence of events presented in Figure 1: A *triggering event* (e.g. sensor failure) has an *effect on the automation* (e.g. mode change). This leads to an *inappropriate command* for pitch or thrust. The inappropriate command occurs while the aircraft is experiencing a relative *deceleration* to the minimum safe operating speed. The relative deceleration is the result of either the aircraft decelerating to a fixed minimum safe operating speed or a change in the minimum safe operating speed (e.g. due to ice contamination on the wing). Finally, the flight crew *fails to intervene* to arrest the deceleration through the minimum safe operating speed and into controlled flight into a stall (CFIS).

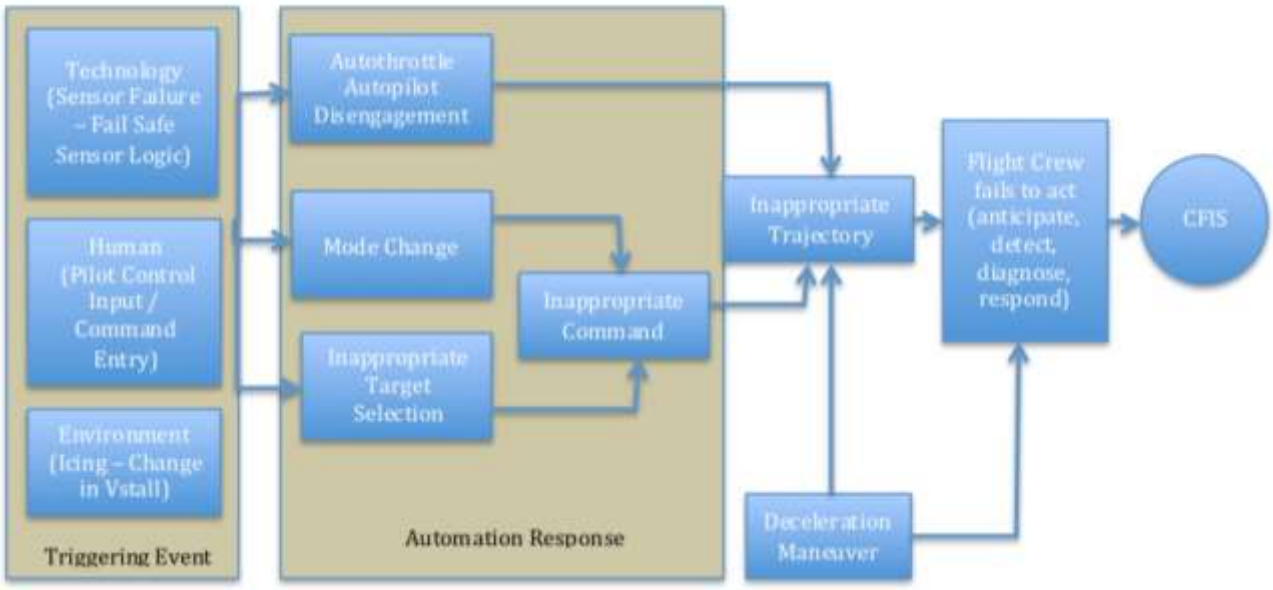

Figure 1. Sequence of Events Leading to Controlled Flight Into Stall (CFIS)

Phase of Flight

The CFIS events occurred in all phases of flight. Six accidents occurred while the aircraft were climbing to the cleared altitude with maximum thrust. In one case (Midwest 490), the flight crew had selected a fixed rate-of-climb at an airspeed that could not be maintained even at maximum thrust. In all the other CFIS cases that occurred during climb, errors in airspeed resulted in inappropriate commands. One accident occurred during cruise. Two accidents occurred during descent and 9 occurred during approach. The accidents that occurred during cruise involved sensor failures that could not be handled by the automation. The automation disengaged, transferring control of the flight trajectory to the flight crew. However, the flight crew was faced with the same inaccurate sensor data that caused the transfer of control and failed to regain control of the aircraft. All the descent and approach cases involved level flight or fixed rate of descent in which the thrust setting was too low to maintain the desired airspeed (e.g. XL Germany 888T, Colgan Air 3407) or the autothrottle was disengaged and no longer controlling airspeed (e.g. AAL 903) or a mode change occurred to a mode that no longer actively controlled to the target airspeed (Asiana Air 214, TA 1951).

Triggering Events

Sensor failures and failures in the associated sensor fail-safe logic were the most common triggering events (see Table 1). However, there was no single sensor-type or class of failure that was common to all of these cases. Sensors that experienced failures included: angle-of-attack sensors (XL Germany), pitot tubes (AF 447, Midwest 490, BirgenAir 301, NWA 6231), and radio altimeters (TA 1951). Further, the fail-safe sensor logic included both voting mechanisms that select the perceived non-failed sensor, as well as averaging mechanisms that average sensor inputs. Changes in aerodynamic characteristics of the aircraft due to icing conditions contributed to three accidents (Colgan Air EWR/BTV, Midwest 490, American Eagle 3008). Flight crew errors contributed to six accidents (Colgan Air EWR/BTV, Colgan Air 3407, United Express 629, KingAir Evereth, Asiana Air 214, Provincial Airlines). For example, the flight crew of Asiana Air Flight 214 inappropriately selected Flight Level Change (FLCH) mode during the approach (NTSB, 2013b). The selection of FLCH resulted in a change to a "dormant" autothrottle mode in which the autothrottle no longer controlled to the airspeed target. In some cases, the triggering event was not identified (AAL 903, ThomsonFly Bournemouth, ThompsonFly Belfast).

Effects of Triggering Events on the Automation

The triggering events had a variety of effects on the automation. When the triggering event was a sensor failure, there were four types of effects on the automation: 1) the automation disengaged (e.g. Air France 447), the

automation mode changed (e.g. Turkish Airlines 1951), 3) the target used for control was calculated incorrectly (e.g. XL Germany T888), or 4) the generated command for pitch or thrust was inappropriate for the current maneuver (e.g. BirgenAir 301).

Table 1.

CFIS Events by Category of Triggering Event and Effects of Triggering Events on the Automation.

Category of Triggering Events	**Effects of Triggering Events on Automation**	**CFIS Accidents/Incidents**
Sensor failures and associated fail-safe sensor failure logic	Disengagement	AF 447, Provincial Airlines, Midwest 490, AAL 903, Air France 447
	Mode change (A/T) Moded-Input Device mode change (Throttle Levers)	Asiana Air 214, TA 1951
	Target error	XL Germany
	Command error	Iceland Air 662, Midwest 490, Provincial Airlines, BirgenAir 301, NWA 6231
Changes in the aerodynamics of the aircraft	Stall speed calculation	Colgan Air/EWR-BTV, American Eagle 3008
Flight crew entry		Colgan Air EWR/BTV, Colgan Air 3407, United Express 629, King Air Eveleth
Unknown events		AAL 903, ThomsonFly Bournemouth, ThompsonFly Belfast, ThomsonFly/no location specified

Automation Response

The effects of the automation changes were to generate three different types of commands: (1) inappropriate thrust, (2) inappropriate pitch, or (3) autopilot disengagement. In seven cases, the autothrottle did not acquire the desired airspeed target (e.g. TA 1951). In four cases, the automation commanded an unexpected pitch-up that led to airspeed decay (e.g. BirgenAir). In one case, the automation terminated engagement and transferred control of the aircraft to the flight crew (AF 447).

Response Decision

There was no single flight crew response to the events that led to the CFIS accidents that would have been appropriate in all cases. There were a variety of correct responses. These responses can be categorized by the required change in flight crew actions and the appropriate degree of automation to use in the maneuver. In several accidents (XL Germany, Midwest 490, Provincial, ThomsonFly-Bournemouth, ThompsonFly - Belfast, and BirgenAir) the accident reports identify interventions in which the recommended procedure would have been to abort the maneuver being executed and transition to an alternate safe procedure. These interventions include aborting approaches by performing a Go Around (ThomsonFly - Bournemouth, ThomsonFly-Belfast) and terminating a climb or descent and level off (XL Germany, Midwest 490, Provincial, BirgenAir 301). In other cases, the accident reports suggest that it would have been possible to continue with the maneuver being executed with a manual over-ride of the auto-flight system (Colgan Air-Burlington, Colgan Air-Buffalo , Turkish Airlines 1951, United Express 629). In other cases (AAL 903), a manual mode/target selection followed by auto-flight system re-engagement would have been appropriate. In hindsight, the lack of airspeed information in two accidents (AF 447 and NWA 6231) predicated aborting the existing procedure and resorting to a "pitch-and-power" maneuver (i.e. wings level, pitch - 5 degrees up, power - 75% thrust).

The decision making required to identify the appropriate response frequently was not supported by the available automation cues. This decision must be based in part on the confidence that the flight crew has in the status of: 1) the aircraft structure and airfoils, 2) the aircraft sensors, 3) the control surface and propulsion systems, and 4) the automation. As the events leading to the CFIS accidents unfolded, the degree to which the automation was functioning, the status of the sensors, and the degree to which other aircraft systems may have been degraded would not have been obvious to the flight crew.

The execution of the appropriate intervention response was hindered in some cases by *moded input devices* that behaved differently under different circumstances. For example, in the aircraft involved in the TA 1951 accident, the throttle levers operate with two modes of operation. In the "airborne mode," the throttle setting can be manually over-ridden and will hold the manually set thrust setting. In the "land mode," the throttle setting can be manually over-ridden, but the thrust setting will automatically retard to idle unless a pilot holds the throttles in position. In the Asiana 214 accident, the pilot overrode the throttle setting by manually repositioning the throttles, but expected the autothrottle to advance to maintain airspeed. However, the act of repositioning the throttles resulted in the autothrottles entering a dormant mode. In these aircraft, the state of the autothrottle mode is not clearly annunciated on the flight deck.

General Discussion

Normal Accidents and Functional Complexity Failures

Studying a series of accidents across domains (i.e. nuclear power plants, aircraft, ships, petrochemical processing plants), Charles B. Perrow (1984), identified a phenomenon he labeled "Normal Accidents." These accidents were characterized by a failure that was the result of the interaction of functions with complex behaviors within a tightly coupled complex system. Perrow argues that in complex systems it is inevitable that the system occasionally will yield behavior that is inappropriate in certain circumstances and surprising to operators. For example, the system designers may not have considered particular combinations of input conditions that may occur in unusual circumstances. Alternately, the system itself may generate rare combinations of intermediate states that are not covered by the design. In these "functional complexity failures" there is no single point of failure. The automation behaves as it was designed, but the functional complexity results in a failure.

The CFIS accidents described here fit the characteristics of the "Normal Accident." In all of these cases, a structurally and mechanically sound aircraft was flown into an aerodynamic stall. Although a deceleration through $1.3V_{Stall}$ and then through V_{Stall} occurred in each accident, there is no pattern or consistent failure in the types of triggering events, in the effects of the triggering events on the automation, or in the inappropriate commands generated by the automation. The source of the failure is a complex interaction between factors.

To address functional complexity failures, one must examine the human-automation system as a whole. The concept of operations for the "flight deck system" is for the flight crew to delegate tasks to the automation and to supervise its performance. In the event that the automation generates an inappropriate command (e.g. throttles maintain idle thrust when the crew expects them to advance), the flight crew is expected to intervene. However, the ability of the flight crew to detect these rare events and to act appropriately is severely compromised by two different factors: 1) the knowledge required may not be present in the system and 2) the knowledge in the system is not properly communicated among the components.

Gaps in Flight Deck Knowledge to Respond to Functional Complexity Failures

Modern aircraft automation is inherently complex. It must be to deal with the complexity of the technology and operational environment. It is not feasible to train pilots to understand the *complete* behavior of the automation. The system itself is constructed by teams of engineers across a geographically dispersed supply chain, none of whom can be completely conversant with the behavior of the entire system. Hence, it is not surprising that pilots frequently do not fully understand their automation. Indeed, it would be impossible to provide pilots with a detailed knowledge of the automation. However, it may be possible to provide pilots with a functional knowledge of the automation. Current automation training is focused largely on learning procedures and not on developing a broad understanding of the automation. This leaves pilots with many gaps in their knowledge which they may plug with simplified behavioral models or misconceptions. In some cases, pilots may not even understand how commonly used procedures work and why potential alternative procedures would not.

But "automation education" by itself could not have prevented all of the CFIS incidents studied here. It is simply not reasonable to expect pilots to be able to learn all of the potentially useful information about their aircraft automation and to be able to recall it when needed. For example, in the Turkish Airlines 1951 accident, the pilots would have had to remember (without any cues) that one of the automation sub-systems (i.e. the auto throttle) relies on the Captain's radio altimeter only to determine altitude and select the active mode. Typically, auto-flight

functions may be shifted from position to position (e.g. Captain's side to First Officer (F/O) side) so that when the FO is flying, most auto-flight systems rely on equipment on the FO's side -- but not in this case. Furthermore, the model of aircraft involved in the accident has two substantially different "RETARD" modes. While at altitude, "RETARD" will allow pilots to override the autothrottle by manually repositioning the throttle levers. However, when the aircraft is in the landing flare, "RETARD" will automatically reposition the throttles to idle. In addition, the Captain's radio altimeter on this particular aircraft had a history of maintenance issues, and hence might need to be monitored carefully.

In this case, the Captain's radio altimeter malfunctioned generating a value that showed that the aircraft had landed while it was still at 2000' above ground level. With the FO in command, the flight deck configured with the automation on the F/O's side, and the FO's radio altimeter functioning properly, the aircraft decelerated on the approach and the automation entered a "RETARD" mode as expected. However, because of the Captain's malfunctioning radio altimeter, the auto-flight system behaved as if it were in the *landing flare*, retarding the throttles to the idle position. When the FO pushed the throttles forward to arrest the deceleration, the automation returned them to idle. There is little doubt that had the pilots been briefed about these issues immediately prior to the flight, they would have remembered all of the relevant information during the approach. However, pilots are inundated by information from the Flight Crew Operating Manual (FCOM), Federal Aviation Regulations (FARs), flight training manuals, manufacturer's bulletins, "read-before-flight" memos, dispatch briefings, etc. In this context, it is unlikely that pilots would be able to retrieve the information relevant to a particular rare event months or years after they encountered it. The required knowledge is effectively not in the system.

Mitigation with Decision Support Tools

It is possible to provide some support. Sufficient automation education could be provided so that pilots would have substantial foundational knowledge and would know enough to ask the right questions. Then, computerized memory support tools could be used to provide the required information when needed. For example, when the aircraft serial number is entered before a flight, the on-board computer support tool could retrieve information about the aircraft maintenance history and provide implications of that history for the operation of the flight.

However, access to this knowledge is not sufficient. To determine what to do in any particular situation, pilots need to understand the current state of the aircraft. In the situations studied, this understanding was frequently lacking. Often, this occurred because the automation did not provide the necessary information. For example, in several cases, the automation disengaged when sensor input became unreliable. However, the same unreliable information was provided to the pilots who are in no better position than the automation to use this information.

In these situations, in very short order, pilots must determine why the automation disengaged. If it disengaged because sensor information became unreliable, the pilots must determine what information is reliable and what to do to regain control of the aircraft. Sometimes it is not clear what information is reliable and what information is not – this is especially difficult with sporadic failures and multiple displays that appear to reference independent sources but do not. In other cases, the information provided was ambiguous. Particularly problematic is information about the functioning of the auto-flight system. For example, the "RETARD" mode label described above refers to two substantially different functions. In general, the Flight Mode Annunciator (FMA) does not provide the information needed to properly supervise the aircraft automation and evidence suggests that pilots generally spend little time looking at FMA (Sarter et al., 2007; Björklund et al., 2006).

To properly supervise automation, pilots need to know: 1) what is controlled by each automation mode, 2) where each mode obtains data about the current state of the aircraft, 3) where each mode obtains targets, and 4) what actions each mode will take when the target is achieved. But having this knowledge is not sufficient. It merely provides a general framework. At every point during the flight, the framework must be populated with current information about the state of the aircraft and how it relates to the intended flight path. This requires that pilots: 1) know where to find the relevant information, 2) attend to these sources, 3) interpret the information correctly, and 4) integrate this information with their stored knowledge of the automated flight system and intended flight path. The requisite information is generally available somewhere on the flight deck, but it is not necessarily easy to find; it may be scattered between the PFD, MCP, ND, CDU, ECAM, and sometimes stand-alone thrust displays.

The cockpit of the modern airliner is a hybrid design. It incorporates the shell of an automated vehicle on top of that of an older manual aircraft design. Neither this design nor the training that accompanies it fully embraces the concept of the pilot as the supervisor of an integrated system. Instead, the pilots are alternately treated as passengers, data entry units, and barnstormers from an earlier era. Providing pilots with fundamental knowledge of the aircraft automation and clear information about the integrity of the sensor information and current status of the aircraft automation and its intentions would have averted the great majority of the CFIS accidents studied. However, this requires an appreciation of the role of the pilot in the modern commercial airliner and a willingness to make fundamental changes in our concepts of how aircraft automation should interact with pilots in this complex system.

Acknowledgements

This work was funded in part by NASA NRA NNX12AP14A and internal GMU Research Foundation funds. Thank you for technical suggestions from Immanuel Barshi, Michael Feary, Randy Bailey, Paul Krasa, Steve Jacklin, Houda Kourdali, Julia Trippe, George Dononhue, Akshay Belle, John Shortle, Mike Hieb, Paulo Costa, and Yong Tian.

References

Bayuk, A.J. (2008) Aviation Safety Management Systems as a Template For Aligning Safety with Business Strategy in Other Industries. American Society of Safety Engineers - The Business of Safety: A Matter of Success Symposium. Baltimore, Maryland, march 13-14, 2008.

Björklund, C., Alfredson, J., & Dekker, S. (2006). Mode Monitoring and Call-Outs: An Eye-Tracking Study of Two-Crew Automated Flight Deck Operations. International Journal of Aviation Psychology, 16, 257-269.

IATA (2013). IATA Safety Report. 49th Edition issued in April 2013. 800 Place Victoria, PO Box 113, Montréal, Quebec, H4Z 1M1.

ICAO (2013). 2013 Safety Report. International Civil Aviation Organization, 999 University Street, Montréal, Quebec, Canada, H3C 5H7.

Perrow, C. (1984). Normal Accidents. Basic Books, New York.

Sarter, N., Mumaw, R., & Wickens, D. (2007). Empirical Study Combining Behavioral and Eye-Tracking Data. Human Factors: The Journal of the Human Factors and Ergonomics Society, 49, 347.

Sherry, L. R. Mauro, I. Barshi & M. Feary (2014) Mitigating Controlled Flight in Stall Accidents. Internal Report, Center for Air Transportation Systems Research, George Mason University (CATSR-007-2013)