MITIGATING FUNCTIONAL COMPLEXITY FAILURES: DESIGNING THE OPERATOR INSIDE THE VEHICLE OODA-LOOP

Lance Sherry, Center for Air Transportation Systems Research at George Mason Univ., Fairfax, VA.
Robert Mauro, Decision Research Inc. & University of Oregon, Eugene, OR.

Abstract

A class of aircraft accidents and incidents, known as Controlled Flight into Stall (CFIS), are characterized by a structurally, mechanically, electronically sound aircraft that is commanded by the automation to fly into the onset of an aerodynamic stall. These accidents are not the results of failed components; instead, they occur as a result of the complexity of the behavior and architecture of the automation that under rare circumstances results in an inappropriate command. This type of "failure," is known as a Functional Complexity Failure (FCF). One of the most pernicious characteristics of FCFs is that they are difficult for operators to detect and intervene (i.e. they "start a fire and simultaneously turn off the fire alarm"). Researchers studying the CFIS accidents have proposed specific point-fixes to the automation to assist in preventing a specific FCF or by alerting the flight crew in these scenarios (e.g. energy-situation awareness, low speed alerting, etc). Without a holistic view for combating FCF's, these solutions are simply fighting battles in the last war.

This paper describes a holistic approach to analyzing the manner in which FCFs occur and how to mitigate them. The novel approach described in this paper is to conduct a *thought experiment* in which the flight crew and automation are treated as adversaries in an Observe-Orient-Decide-Act (OODA) Loop. This analysis shows how in an FCF, the automation deploys techniques (e.g. creating complacency, uncertainty and disorder, hidden intentions, deception, and distraction) to get "inside" the flight crew OODA-loop. A holistic mitigation approach is described to design the automation to ensure that the operator is always inside the vehicle's OODA loop .

INTRODUCTION

In the seminal book on modern accidents, Charles Perrow [1], identified a form of accidents in modern complex technological systems that is "inevitable" and that have the potential to result in catastrophic hazards. These accidents, which Perrow labelled "normal accidents," are characterized by an inappropriate calculation of a parameter that initiates a series of events in behaviorally complex, tightly coupled systems. These events lead directly to commands by the automation to lead the system into unsafe operating regions. One of the characteristics of these scenarios is that the series of events are difficult to detect. As Perrow put it, they "start the fire and simultaneously turn off the fire alarm," preventing operator detection and intervention.

One type of normal accident that has occurred repeatedly in aviation is Controlled Flight into Stall (CFIS) [2]. In CFIS accidents a structurally, mechanically, electronically sound aircraft is commanded by the automation to fly into the onset of aerodynamic stall. In all of the accident scenarios studied, the flight crew was not able to intervene.

A detailed study of the CFIS accidents determined that although the hazardous event (i.e. onset of stall) was the same for all the accidents, the events leading up to the inappropriate command were unique for each accident. These events were the result of complex logic in a tightly coupled system that led from an inappropriate calculation in a sensor or unusual pilot entry for a phase of flight, to an inappropriate command. This phenomenon, in which a system failure occurs although no component breaks or fails, has been labeled a *Functional Complexity Failure* (FCF).

Researchers studying CFIS accidents have proposed excellent point solutions focused on particular stages in the individual accident scenarios. These point scenarios include low speed alerting [3], energy-state awareness [4], and mode checking [5]. However, these approaches may provide solutions for particular accident scenarios but they do not anticipate possible future CFIS accident scenarios. Further, typical human factors inspection methods are designed to uncover user-interface design characteristics (e.g. tactile, visual salience), and on human-automation interaction (e.g. task analysis) problems. They are not designed to discover system level problems. It requires a high order of engineering discipline in application of these approaches to detect the system failures and to devise interventions for FCFs.

This paper describes a holistic analysis of the FCF for CFIS and derives a holistic mitigation approach. The novel approach described in this paper is to conduct a *thought experiment* in which the flight crew and automation are treated as adversaries using an Observe-Orient-Decide-Act (OODA) Loop to achieve tactical advantage. The analysis shows how in an FCF scenario, the automation deploys techniques (e.g. creating complacency, uncertainty and disorder, false intentions, deception, and distraction) to get "inside" the flight crew OODA-loop and surprise the crew with a CFIS. A holistic mitigation approach to counter the automations deceptive techniques is described.

The paper is organized as follows: Section 2 provides an overview of FCFs and CFIS accidents. Section 3 describes the OODA-Loop and techniques for creating tactical advantage. Section 4 describes the analysis of FCFs for CFIS using the OODA-Loop framework. Section 5 describes the holistic mitigation approach for FCFs.

FUNCTIONAL COMPLEXITY FAILURES AND CONTROLLED FLIGHT INTO STALL

The execution of a revenue-service airline flight is achieved by execution of a sequential set of navigation procedures (e.g. departure, jetways, standard arrival procedures, approach procedures, …). These procedures are designed to ensure terrain and obstacle avoidance, and coordinate traffic with Air Traffic Control for collision avoidance. To achieve the desired trajectory for each navigation procedure, the aircraft performs a series of maneuvers. Each maneuver requires careful coordination of the airplane's energy to maintain a lift generating energy-state at all times.

The desired aircraft trajectory is achieved by coordinated adjustment of the airplane pitch, roll and thrust. This is not a trivial activity as pitch, roll and thrust must be coordinated to remain inside the aircraft speed envelope and maintain a safe-energy state.

To assist the flight crew in performing this fatiguing task, guidance and control automation has been introduced onto the flight deck. The Autopilot (A/P) directly controls pitch and roll in concert with an Autothrottle (A/T) that controls thrust. The altitude, airspeed, course/heading and rate-of-climb/descent targets that are used as the reference by the A/P and A/T can be set manually by the flight crew via a Mode Control Panel (MCP) or automatically by the Flight Management System (FMS). When the Flight Management System (FMS) is engaged (i.e. VNAV and/or LNAV are engaged), the FMS automatically sets a coordinated sequence of targets and control strategies for the A/P and A/T to achieve the sequence of navigation procedures "programmed" by the flight crew into the FMS.

The automatic switching of targets and control strategies by the automation has proven to be a challenge for the flight crews tasked with monitoring the automation for conformance to the navigation procedure and avoiding the hazards of flight (e.g. terrain, traffic, and speed envelope violations). This challenge has been called Mode Confusion [6] or Automation Surprise [7], [8], [9], and has been identified as a contributing factor to aviation accident and incidents [10], [11], [12].

The FCF for the CFIS scenario is summarized in Figure 1, is as follows

Triggering events are varied with no two accidents with the same trigger. Triggering events are categorized by: (1) sensor data discrepancies that are mischaracterized by the sensor fail-safe logic, (2) inappropriate pilot entries, and (3) environmental conditions that change the aerodynamics of the aircraft (e.g. icing).

Aircraft enters an appropriate maneuver to decelerate to the minimum safe operating airspeed, or enters this maneuver at some later time.

Automation is affected by the triggering event such that the automation is no longer actively controlling airspeed. This is manifested in two ways: (1) the automation is decoupled (e.g. Autothrottle disengages), or (2) the automation selects a control mode that no longer actively controls speed (e.g. dormant throttle mode, land mode).

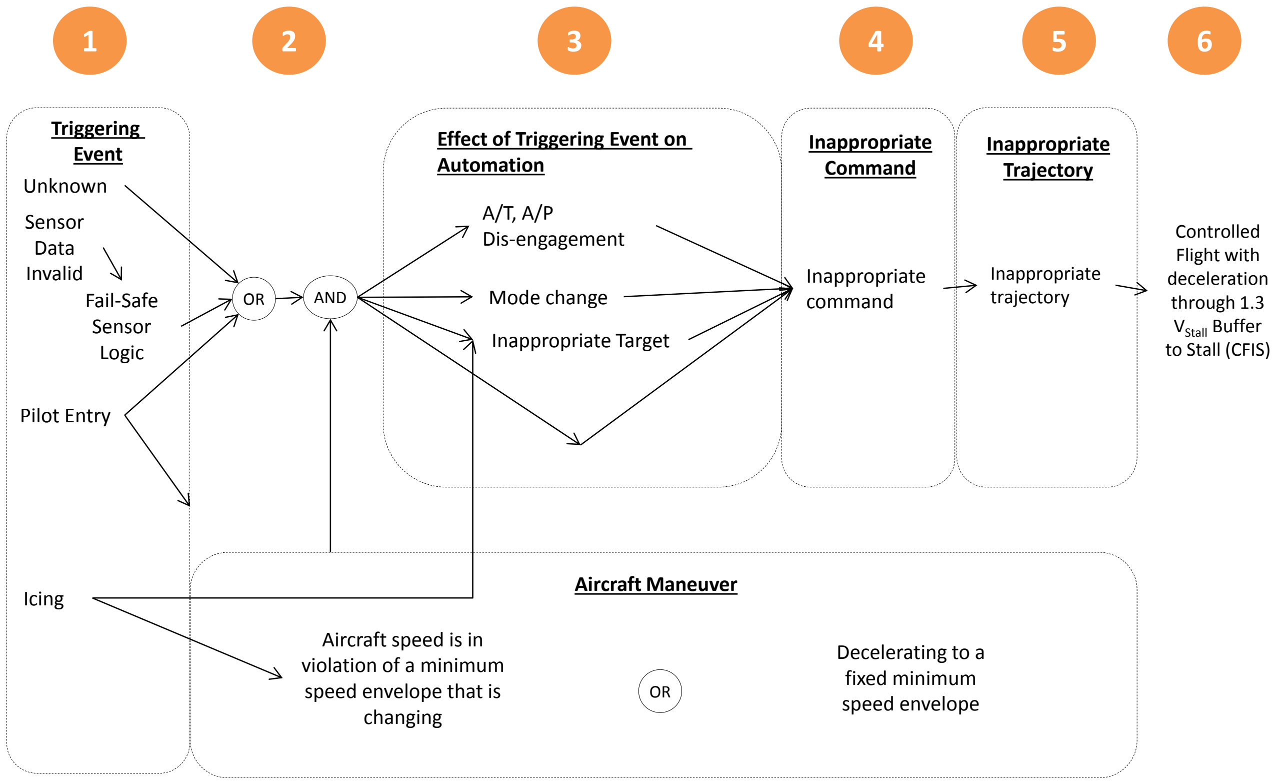

FIGURE 1: Functional Complexity Failure (FCF) for the Controlled Flight into Stall (CFIS) scenario

The automation provides inappropriate commands to fly aircraft into the onset of the stall

The aircraft therefore flies an inappropriate trajectory into the onset of the stall

At every step in this process, the action is appropriate given the input. There is no single failure that causes the problem. However, the result is a catastrophe – a Functional Complexity Failure.

Furthermore, in all the CFIS accidents studied the flight crews were unable to recognize the CFIS scenario and intervene in a timely manner. This occurred in part because the flight deck automation is not designed to support the intervention task [13]. Since the triggering event was not a technical error or component failure, there was no annunciation of this condition. Likewise the mode changes were "masked" by overloaded mode labels, or ambiguous Flight Mode Annunciations (FMA). The commands and trajectories were also "masked" by the correct pitch and thrust commands for an appropriate decelerating maneuver.

THE OODA –LOOP AND TECHNIQUES FOR ACHIEVING TACTICAL ADVANTAGE

The OODA-loop framework describes a cyclical sequence of activities used to gain tactical advantage over an adversary [14]. The framework was developed by military strategist USAF Colonel John Boyd in the context of a fighter-jet "dog fight." The framework has subsequently been applied to litigation [15], business [16], and sports.

The OODA-loop refers to a continuous cycle of (1) observe, (2) orient, (3) decide, and (4) act. The loop is initiated by *observation* of the adversary. This information is assessed and interpreted to determine the intentions of the adversary (i.e. *orientation*). Based on the orientation information, *decisions* are made and then executed (i.e. *act*). The loop is then executed again with updated observations, assessments, and interpretations of intention, decisions and actions. The loop applies to long cycle times in strategic planning, shorter cycle-times in tactical planning, and instantaneously in real-time operations.

For example, consider a simple fighter jet dog-fight. Before the adversary is in visual contact, the fighter pilot is observing and orienting to achieve tactical advantage (i.e. higher altitude and in the adversaries line-of-sight to the sun). As the adversary comes into radar contact, additional information about the aircraft and it's performance capabilities as well as the trajectory and intentions of the adversary are taken into account and decisions acted upon to increase tactical advantage. As the adversary is engaged, tactical advantage is sought by anticipation and by deception in actions.

The underlying principle for achieving tactical advantage is to use a better understanding of the unfolding situation to set up its opponent by employing actions that fit with the opponent's expectations, which Boyd, following Sun Tzu (trans. 1988), called the *cheng*. When the time is ripe, it springs the *ch'i*, the unexpected, extremely rapidly.

When an adversary's actions cause surprise and force their foe to change plans, they have achieved the tactical advantage of "*getting inside*" the foe's OODA-loop. OODA-loop practitioners have outlined the following techniques to achieve *cheng* and spring the *chi'i*:

1. Create complacency – set up the adversary by behaving in repeatable patterns
2. Hide intentions
    a. Keep intentions hidden at all times
    b. Allow the adversary to see actions, especially those actions that are associated with more than one intention
    c. Use deception to hide the true intentions of actions and to "assist" the adversary to interpret the actions to reach an incorrect interpretation of the adversary's intentions
3. Use distractions to absorb the adversary's resources
4. Block corrective actions.

Uncertainty and disorder play a significant role in the outcome. They limit the degree to which the adversary's actions can be anticipated. The ability to analyze uncertainty better than the adversary provides a window of opportunity to achieve tactical advantage.

ANALYSIS OF CFIS ACCIDENTS USING THE OODA-LOOP FRAMEWORK

Example CFIS Accident – Turkish Airlines Flight 1951

On February 25, 2009 Turkish Airlines Boeing 737-800 designated as Flight 1951 departed from Istanbul, Turkey bound for Amsterdam, Holland. As the flight approached Amsterdam Schiphol airport it was assigned the "Polderbaan" approach for runway 18R for landing. With the First Officer flying, the aircraft was vectored to intercept the localizer at approximately 6nm from the runway (about 2nm closer to the runway than normal). Shortly after acquiring the runway centerline, it was cleared to descend below 2000'.

As a result of the ATC vectoring, the aircraft was "high and fast." Thus, it was required to decelerate quickly to the reference landing speed and to descend rapidly to the desired three degree descent glideslope to the runway. To achieve this goal, the automation commanded the aircraft to perform a descending trajectory to acquire and maintain the glideslope. Simultaneously, the automation commanded the throttles to idle thrust while the aircraft decelerated to the reference landing speed.

At this point, the flight was progressing like many that the pilots had flown before. There was nothing to indicate that anything was amiss. However, unbeknownst to the pilots the Captain's radio altimeter (RA) had malfunctioned. As the aircraft descended through 1950 feet, the altimeter registered -8 feet. In response, the autothrottle transitioned to the "retard flare" mode, as all the conditions for the mode transition appeared to be present (e.g. near the ground, flaps 15). This mode is designed to automatically decrease thrust shortly before touching down on the runway at 27 feet above runway height. Thus the automation commanded the throttles to the idle, but with the throttles already set to idle the effect of this mode transition went unnoticed. At this time, the automation's intention was to no longer to control airspeed. However, this intention was disguised. The aircraft was descending and decelerating as anticipated. There was no reason to expect that this approach would be any different from those that had come before.

But what about the FMA? Why didn't it alert the pilots to the change in mode? Indeed, the FMA did indicate that the autothrottle was in "RETARD" mode. However, on this aircraft there are essentially two modes labeled "RETARD." While in flight, the RETARD annunciation indicates that the autothrottles are set to reduce thrust to allow the aircraft to decelerate with the intention of advancing thrust as the aircraft reaches the desired target speed. During the landing sequence, the RETARD annunciation indicates that the autothrottles are locked at idle. In this mode, if the throttles are manually disturbed, the automation assumes that the pilots are making a minor adjustment and will return the throttles to idle once the pilot releases the handles. Thus, the throttle position, aircraft behaviors, and FMA annunciation all disguised the automation's true intentions.

What about the anomalous RA reading? If the Captain had noticed this discrepancy, he might have been alerted that something was amiss. However, the First Officer was the Pilot Flying (PF) and the triple-redundant autopilot and dual autothrottles were selected on the First Officer's side. The RA on the First Officer's side was correct and matched the barometric altitude readings as well as the view outside the flight deck window. From the PF's perspective, there was no indication that anything was wrong. The automation did not explicitly alert the crew about the discrepancy between the RAs on the Captain's and First Officer's sides. It also did not share the results of the "fail-safe" logic that selected the Captain's side as the "correct" reading and provided this information to the autothrottle. The automation intended to use the Captain's RA but hid this from the pilot flying.

The automation did issue one warning: "TOO LOW! GEAR!" Due to the low reading on the Captain's radio altimeter, the flight deck sounded an audible warning signal indicating that the aircraft's landing gear should be down. However, to the pilots this appeared to be an error, as the aircraft was at an appropriate altitude and the automation was clearly performing the descent and glideslope acquisition flawlessly.

As the aircraft approached the desired reference landing speed (144 knots), the automation did not command the throttles to advance to acquire and maintain the desired airspeed. Instead, the automation continued to allow the aircraft to decelerate. At 144 knots, the pilots manually increased thrust to sustain that speed. However, because the autothrottle, was in the "retard flare" mode, it immediately returned the thrust lever to idle because the first officer did not hold the throttle lever in position. The autothrottle deceptively changed the behavior of the input device (i.e. the Throttle Levers) without any annunciation of the change. The aircraft decelerated to 83 knots before an aerodynamic stall at 490 feet lead to a crash approximately 1 mile from the runway. There were eleven fatalities, nine passengers and all three pilots.

In this accident, the automation acted like a clever adversary, luring the pilots into believing that it intended to use the throttles to control airspeed as it had done many times before. But on this occasion, the failure of the Captain's radio altimeter caused the automation to have a different intention. Like a clever adversary, the automation hid this intention from the pilots disguising it behind misleading actions and indications. The pilots were never able to get inside the OODA loop.

OODA Tactical Advantage Analysis of Turkish Airlines Flight 1951

As a thought-experiment, using the framework of the OODA-Loop, how did the automation gain tactical advantage over the flight crew?

Create Complacency

The automation routinely performed the task of approach and landing flawlessly. A flight crew may never see the FCF/CFIS phenomenon in their careers. Also, apart from the late vector and descent clearance (which though not standard is not uncommon), this flight was not unusual and appeared to the flight crew to be "just another landing."

Hide Intentions

During the approach, the Captain's Radio Altimeter (RA) erroneously displayed 8191 feet (the maximum possible value). When the aircraft descended through 1950 feet, the RA suddenly displayed negative 8 feet. This reading caused the Autothrottle, by design, to revert to the "retard flare" mode as all the conditions for the mode transition were present (e.g. near the ground, flaps 15). The Retard mode is designed to automatically decrease thrust shortly before touching down on the runway at 27 feet above runway height. The throttles retarded to the idle positioning commanding the thrust to the approach idle setting. At this time, the automation's intention was to no longer to control airspeed.

Deception #1

During the descent and capture of the glideslope, the First Officer (FO) was the Pilot Flying (PF) and the triple-redundant Autopilot and dual Autothrottles were selected on the First Officer's side. The RA on the First Officer's side was correct and matched the barometric altitude readings as well as the view outside the flight deck window. From the FO's perspective, there was no indication that anything was amiss. The automation did not explicitly alert the discrepancy between the RA on the Captain's and First Officer's sides. It also did not share the results of the "fail-safe" logic that selected the Captain's side as the "correct" reading and provided this information to the Autothrottle. The automation intended to use the Captain's RA but hid this from the FO.

Deception #2

The autopilot flawlessly captured and maintained the glideslope. The Autothrottle, however, had quietly transitioned to the "retard flare" mode. In this mode, the Autothrottle commanded an idle thrust setting, which was the appropriate action during the deceleration to the reference landing speed (144 knots). However, this mode does not advance the thrust to hold the desired airspeed target. In this way the command and the subsequent deceleration to 144 knots was what was to be expected.

In addition to the expected commands, the Autothrottle annunciated RETARD on the Flight Mode Annunciation (FMA). This reflected the transition of the Authothrottle to the 'retard flare' mode. The RETARD label, however, is deceptive. It is used while the aircraft is airborne when the throttles retard to the idle stop *and* when the 'retard flare' mode is active for the flare maneuver. The RETARD label was an appropriate annunciation with the throttles at the idle stop while the aircraft decelerated to the landing speed with idle thrust but hid the fact that the Autothrottles had no intention of advancing the throttles to hold the airspeed.

Distraction

Due to the low reading on the Captain's radio altimeter, the flight deck sounded an audible warning signal -- "TOO LOW!, GEAR!" -- indicating that the aircraft's landing gear should be down. However, this appeared to be an error, as the aircraft was at an appropriate altitude and the automation was clearly performing the descent and glideslope acquisition flawlessly.

Block Corrective Actions

At 144 knots, the pilots manually increased thrust to sustain that speed. The Autothrottle, however, because it was in the "retard flare" mode, immediately returned the thrust lever to idle power because the first officer did not hold the throttle lever in position. The Autothrottle deceptively changed the behavior of the input device (i.e. the Throttle Levers) without any annunciation of the change.

GETTING INSIDE THE VEHICLE'S OODA-LOOP

The OODA-loop framework described above suggests the general rule that to maintain tactical advantage (TA) over adversaries and not be surprised by their actions, one must get inside the OODA Loop. This is achieved by building insight into their intentions and associated actions. The specific techniques for countering TA for FCF for a CFIS scenario are summarized in Table 1. The strategy is to know the possible intentions and to be able to recognize the markers of all the intentions of the adversary that lead to hazards, especially the intentions that are masked by current maneuvers or hidden by deceptive displays.

Avoid complacency

Complacency may be addressed with appropriate (or focused) "paranoia" with regard to the trajectories that lead to hazards. Decelerating to the minimum safe operating speed anywhere in the flight regime should initiate the flight deck etiquette of a "sterile flight deck" without any distractions. The pilot monitoring should know the conditions under which the automation could silently transition to a non-active speed control and should actively monitor for the markers of these conditions. The modes associated with non-active speed control must be trained and practiced. For example, all "dormant" modes, or non-active speed control modes should be identified in training and practiced. Also, the conditions and cues for automation decoupling should be trained and practiced.

Sherry & Mauro [13] proposed a *Paranoid Pilot Associate (PPA)* concept in which an automated device would follow the aircraft trajectory and based on a data-base of scenarios, would provide a probabilistic alert to the flight crew with specific instructions on identifying the issues that require attention at that time. For example, any time the vehicle is decelerating to a minimum safe operating airspeed, the PPA would alert the flight crew to the CFIS scenario. Another condition that would trigger an alert is any change in sensor status or sensor selection performed by fail-safe sensor logic.

There are several research issues that have to be

TABLE 1: Techniques for Countering Adversary's Tactical Advantage in the CFIS Scenario

Techniques for Tactical Advantage Over Adversary	**Techniques for Tactical Advantage Over Adversary for FCF for CFIS**	**Techniques for Countering Adversary's Tactical Advantage**
Create complacency by behaving in repeatable patterns (i.e. "set-up the adversary)	Fly the maneuver repeatedly without the surprise conditions	Paranoia – expect FCF for CFIS and other hazards and continuously check for FCF scenarios
Keep intentions hidden at all times	Do not annunciate automation intentions directly	Continuously determine present intentions of automation and anticipate next intention. Focus on intentions that can lead to hazards (stall, traffic, terrain). Make intentions the callout.
Allow adversary to see actions, especially those actions that are associated with more than one intention	Fly maneuver with more than one outcome (e.g. deceleration in descent)	Actively look for markers that distinguish action with appropriate intention from actions with inappropriate intentions
Use deception to hide true intentions, and assist adversary in interpreting actions to reach incorrect attribution	Annunciate with functionally overloaded labels	Know functionally overloaded labels and what markers can distinguish underlying modes
Create uncertainty and confusion	Provide erratic data and/or display discrepancies	Actively identify integrity level of flight deck data. Know how to address lower levels of data integrity
Block adversaries response to corrective actions	Switch modes of input device (to prevent intervention)	Anticipate blocking actions by knowing about all moded input devices

addressed including false-positives/nuisance alerts and the communication of uncertainty and rare events. Furthermore, in many cases the information required for this alerting system is not on the aircraft. For example, the maintenance history logs of sensors may not be kept on the aircraft. . In the Turkish Airlines 1951 scenario, the Radio Altimeter had experienced multiple failures in the weeks leading up to the accident. In the XL Germany accident [18], the livery painting and maintenance cleaning required that the protection of the angel-of-attack sensors; blockage of the movement of these sensors triggered the events that led to the accident. Alerts could also be generated for known weather-related problems. For examples, pilots could be alerted about the effects of super-cooled ice crystals on the pitot tubes as the aircraft is about to enter these regions; thus perhaps avoiding the events that led to the demise of Air France 447 [19].

Sherry & Mauro [13] have proposed a Cyber-Sense system that provides pertinent non-aircraft information such as maintenance logs, weather, NOTAMS, anecdotes on the specific navigation procedures in the flight plan to the flight crew. These sets of information could also be coupled with manufacturer's bulletins and advisory circulars providing context sensitive advisories. This concept is embodied in the PPA shown in Figure 1.

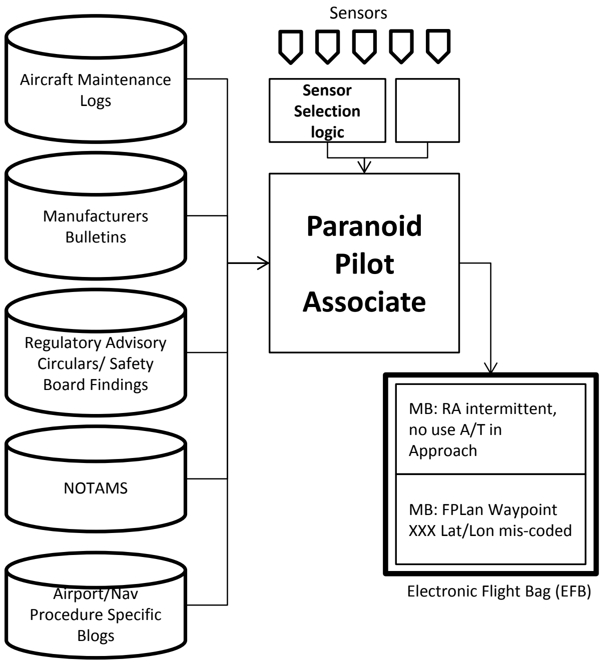
Sensors
Aircraft Maintenance Logs
Manufacturers Bulletins
Regulatory Advisory Circulars/ Safety Board Findings
NOTAMS
Airport/Nav Procedure Specific Blogs
Sensor Selection logic
Paranoid Pilot Associate
MB: RA intermittent, no use A/T in Approach
MB: FPLan Waypoint XXX Lat/Lon mis-coded
Electronic Flight Bag (EFB)

FIGURE 1: Functional Block Diagram of Paranoid Pilot Associate

Understand Intentions

Train automation intentions and display these intentions on the flight deck. Dating all the way back to Aristotle, the communication of intention was considered critical for efficient coordination between autonomous agents. Although in many cases intentions can be accurately inferred from actions, there are situations in which the same actions can be the product of different intentions. Instead of relying on inferences, automation intentions should be displayed on the flight deck [20], [21] (see Figure 2) Experimental results indicate that significant improvements in flight crew awareness of automation actions can be achieved through annunciation of automation intentions [20]. Some of the advantages of these displays may be attainable through enhanced automation training [22].

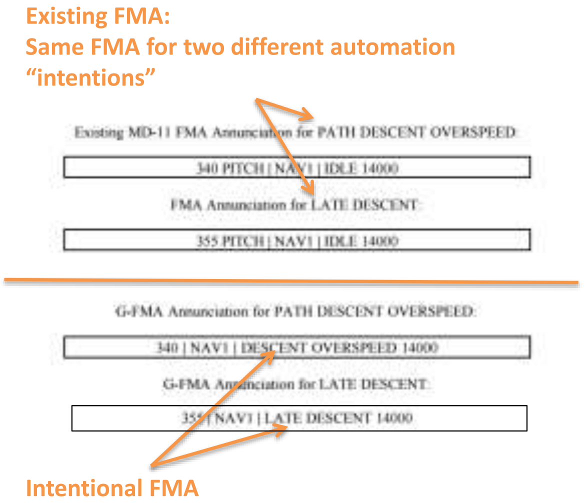
Existing FMA:
Same FMA for two different automation "intentions"
Existing MD-11 FMA Annunciation for PATH DESCENT OVERSPEED
340 PITCH | NAV1 | IDLE 14000
FMA Annunciation for LATE DESCENT
355 PITCH | NAV1 | IDLE 14000
G-FMA Annunciation for PATH DESCENT OVERSPEED
340 | NAV1 | DESCENT OVERSPEED 14000
G-FMA Annunciation for LATE DESCENT
355 | NAV1 | LATE DESCENT 14000
Intentional FMA

FIGURE 2: Example Intentional FMA

The automation's intention to alter thrust or to cease controlling thrust should also be annunciated. Flight plan course changes are displayed on the Navigation Display (ND). Altitude changes are displayed on the Vertical Navigation Display (VND). Some airspeed changes may be displayed if they are associated with speed constraints and speed limits on the ND. Thrust change points are not annunciated. Sherry & Mauro [13] proposed a Thrust Advance Indicator (TAI) display on the Airspeed tape on the PFD. The TIA, shown in Figure 3, identifies the airspeed at which the throttles need to advance to acquire and maintain the airspeed target. The absence

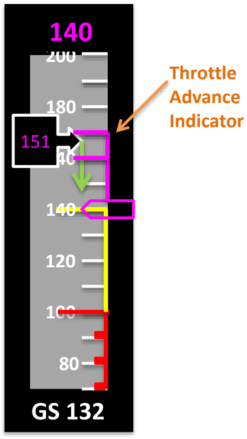

FIGURE 3: During deceleration, Thrust Advance Indicator (TAI) identifies airspeed at which throttles should advance

of throttle movement when the airspeed decreases below the TAI is an indication of a CFIS scenario.

Avoid deception.

The FCF for CFIS specifically results in a situation on which the automation is no longer controlling airspeed. In the CFIS accidents studied there were two categories of scenarios. In the first, the automation transitioned to a mode in which speed was not actively controlled. As noted above, in the TK 1951 accident, the autothrottle transitioned to the "retard flare" mode in which the autothrottle intentionally held the thrust at the idle setting [17]. In the OZ 241 accident, the autothrottle transitioned into a "dormant" state requiring any thrust change to be manually set by the flight crew [23]. In the second scenario, the automation decoupled from the control surfaces/engines. In the AAL 903 [24], ThompsonFly-Bournemouth [25], and AF 447 [19] incidents/accidents, the Autothrottle disengaged.

Speed control status is not explicitly annunciated on the flight deck. Sherry & Mauro [13] have proposed modifications to the PFD to explicitly identify *non-active speed control*. One implementation is to place XXXX's over the airspeed target FMA and airspeed tape. Visual indications could also be provided on the Model Control Panel and Flight Management System (see Figure 4).

Another type of deception is the use of *overloaded labels* for FMA. Exclusive use of labels can be addressed in the design process and trained.

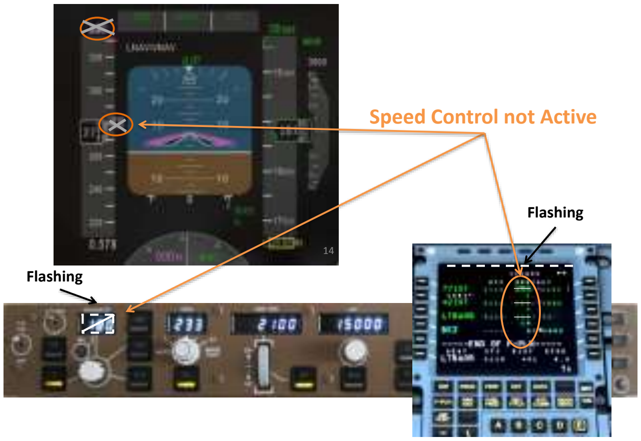

FIGURE 4: Inactive speed control indications on the PFD Airspeed tape, MCP and FMS.

Recognize confusion.

There are several ways in which the automation can create confusion. First, the sensor data may be erratic or discrepant. Attempting to guess in flight which sensors are valid is a difficult task (e.g. AF 447, XL Germany). In some cases, when confronted with confusing sensor indications, it may be prudent to take actions not based on having accurate sensor data such as flying by "pitch-and-power."

Sherry & Mauro [13] proposed a *Data Integrity* (DI) function that monitors sensor status and calculates an index representing the integrity of the sensor data. Sensor discrepancies, sensor fail-safe logic selection of sensors, and/or erratic sensor data are ways in which the DI score would be downgraded. Once the DI score drops below a threshold, flight crews would know to what degree the automation could be trusted.

This idea is embodied in the *Cynefin* framework, developed by Snowden, which characterizes the environment in which a firm operates [26]. In the Simple state, Best Practices are used to sense, categorize and respond. In the Complicated state, Good Practice is used to sense, analyze and respond. In the Complex/Chaotic state, Emergent/Novel practices are used to probe/action, sense, analyze, and respond. The flight deck procedures are not trained this way. The assumption is that the flight crew should always be using Best Practices. However, when the situation is no longer Simple state (e.g. erratic or discrepant sensor data) it should be appropriate to recognize that maintaining the procedure is not an option and the flight deck operations should revert to flying the aircraft, not following the procedure.

Be aware of automation blocking actions

All "moded" input devices should include appropriate annunciation to indicate change in behavior. Further explicit training should be provided to establish the background knowledge to recognize these situations in revenue-service operations.

DISCUSSION

Anxieties about man-made machines is a long-running theme in literature and film. From the legend of the colossal Golem, to Frankenstein, to HAL in 2001: A Space Odyssey, authors have wrestled with the paradox of humans becoming over-reliant on intelligent machines that can turn on their creators in a moments notice. Of course no modern automation has the adaptive ability to evolve to evil intent, however in rare circumstances, the nature of Functional Complexity Failures can appear to intentionally commands and inappropriate behavior while deceiving the operator.

The challenge in designing increased levels of autonomy on the modern flight deck is to understand the role of the flight crew in detecting the inappropriate command.

The modern airliner flight deck, however, is not designed to assist the flight crew to detect and mitigate the ch'i (i.e. surprise). In fact, the current design of the flight deck automation requires the flight crew to monitor for a 10^{-9} hazard reliability for automation designed to a 10^{-5} design assurance standard. Traditional human factors design methods require a high degree of practitioner discipline to address *ch'i* events for FCF. The *gedanken experiment* described in this paper using the OODA-loop, provides a framework for a "hazard analysis" based on the methods used by the automation/vehicle to get inside the flight crews OODA-loop. This method can be applied as Cognitive Walkthrough [27].

Cognitive Walkthrough for Hazard Analysis for Functional Complexity Failures

A method for analysis of flight deck interaction between the flight crew and automation is proposed to address this phenomenon using a cognitive walkthrough [27] style of analysis:

Step 1: Identify *hazard scenarios* (e.g. decelerate through minimum safe operating airspeed).

Step 2: Identify *procedures* for each hazard scenario (e.g. hold entry, approach are associated with hazard decelerate through minimum safe operating airspeed).

Step 3: Identify triggering conditions

Step 4: Identify effects on automation (e.g. *inactive control and/or decoupled automation*) for each segment of the procedure

Step 5: Identify inappropriate commands

Step 6: Identify inappropriate trajectories

Step 7: Identify information available to the flight crew to detect: triggering events, effect on automation, inappropriate commands, and inappropriate trajectories.

Step 8: for each set of information, identify the OODA-loop characteristics that can result in the vehicle getting inside the OODA-loop of the flight crew:

- Complacency
- Hidden intentions
- Actions with multiple intentions
- Deception to hide true intentions, and assist adversary in interpreting actions to reach incorrect attribution
- Uncertainty and disorder
- Blocked response to corrective action (e.g. moded input devices)

Each of these issues with the OODA-loop should be addressed by design changes or

Mitigating Automation Surprise

Automation surprise is first a surprise. We are surprised when events violate our expectations. Surprises are disorienting. It is this disorientation that makes unexpected pleasant events feel more pleasant than similar expected events and that makes unexpected unpleasant events seem more unpleasant. The emotional response of surprise is short-lived, but it may give way to more debilitating responses. Confusion and uncertainty engender anxiety and fear. These are natural reactions to being confronted with a potentially dangerous situation that we do not understand. In our evolutionary past, the physiological and cognitive components of our response to anxiety and fear were adaptive, allowing us to focus on threats and to simultaneously prepare for potential injuries and to take physical action. But in the cockpit, the continued narrowing of attention and the constriction of working memory associated with anxiety and fear interfere with out ability to think broadly and generate creative solutions to complex problems. If the disorienting situation continues without resolution, individuals are likely to become increasingly unable to perform complex mental operations.

We cannot eliminate surprises from aviation, but we can take steps to prevent the negative consequences that may follow. By providing pilots with the information that they need to understand the unexpected situation and the mental framework that they need for understanding this information, surprises can be resolved without allowing the pilots mental capacities to deteriorate as they become increasingly anxious or afraid.

References

[1] Perrow, C. (1984) “Normal Accidents.” Basic Books, New York.

[2] Sherry, L., R. Mauro (2014) Controlled Flight into Stall: Functional Complexity Failures and Automation Surprises. In proceedings 2014 Integrated Communications Navigation and Surveillance (ICNS) Conference, Dulles, Va.. April, 2014. Page D1-1

[3] Avionics Systems Harmonization Working Group Report - Low Airspeed Alerting Systems for Part 25 Aircraft (Final Report). Available 3/30/15 at http://lessonslearned.faa.gov/IndianAir605/ASHWG%20LAA%20Report_15%20March%20Final%20Version.pdf

[4] Kaneshige, J., Benavides, J., Sharma, S., Martin, L., Panda, R., and Steglinski, M. (2014) Implementation of a Trajectory Prediction Function for Trajectory Based Operations. AIAA Aviation Atmospheric Flight Mechanics Conference, No. AIAA 2014-2198, August 2014

[5] Duan, P., M. Miltner, M. Uijt de Haag (2014) A Multiple Hypothesis Prediction Methof for improved Aircraft State Awareness. In Proceedings 33rd Digital Avionics Systems Conference (DASC), Colorado Springs, CO. Oct, 2014

[6] Sarter, N.B., DD Woods (1992) Pilot interaction with cockpit automation: Operational experiences with the flight management system. - The International Journal of Aviation Psychology, 2 (4), 303-321

[7] Wiener, E., R. . Chute, & J. . Moses **(**1999**)** Transition to Glass: Pilot Training for High-Technology Transport Aircraft**,** NASA Contractor Report 1999-208784. NASA Ames Research Center, Moffett Field, CA.

[8] Billings, C.E. (1996) Aviation Automation: The Search for A Human-centered Approach. CRC Press.

[9] Degani, A. (2004) Taming HAL: Designing Interfaces Beyond 2001. Palgrave Macmillan.

[10] Federal Aviation Administration Human Factors Team Report (1996): The Interfaces Between Flightcrews and Modern Flight Deck Systems June 18, 1996. Available 3/31/15 at http://ocw.mit.edu/courses/aeronautics-and-astronautics/16-422-human-supervisory-control-of-automated-systems-spring-2004/readings/interfac.pdf

[11] Australian Bureau of Air Safety Investigation (BASI), August 1999, Advanced Technology Aircraft Safety Survey Report, Flight Safety Digest: Special Issue, Flight Safety Foundation, pp. 137-216.

[12] Commercial Aviation Safety Team, CAST Reports. 2012, Available from: http://castsafety.org/cast_reports.cfm.

[13] Sherry, L., R. Mauro (2014) Design of Cockpit Displays to Explicitly Support Flightcrew Intervention Tasks**.** In Proceedings 33rd Digital Avionics Systems Conference (DASC), Colorado Springs, CO. Oct, 2014

[14] Boyd, J.R. (1976) Destruction and Creation. U.S. Army Command and General Staff College September 1976. Available on 3/31/15 at http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

[15] Dreier, A.S. (2012)Strategy, Planning & Litigating to Win, Boston, MA: Telos Press.

[16] Richards, C. (2004) Certain to Win: the Strategy of John Boyd, Applied to Business. Philadelphia: Xlibris.

[17] The Dutch Safety Board, May 2010, Crashed during Approach, Boeing 737-800, Near Amsterdam Schiphol Airport, Aircraft Accident Report M2009LV0225_01.

[18] BEA (2008) Accident on 27 November 2008 off the coast of Canet-Plage (66) to the Airbus A320-232 registered D-AXLA operated by XL Airways Germany

[19] BE 92009) Final Report on the 1st June 2009 to the Airbus A330-203 Registered F-GZCP Operated by Air France flight AF 447 Rio de Janeiro – Paris.

[20] Feary, M., D. McCrobie, M. Alkin, L. Sherry, P. Polson, e. Palmer (1998) Aiding Vertical Guidance Understanding. NASA/TM—1998-112217

[21] Sherry, L.& P.Polson (1999) Shared models of flight management systems vertical guidance. In The International Journal of Aviation Psychology – Special Issue: Aircraft Automation. L. Erlbaum: N.Y

[22] Sherry, L., M. Feary, P. Polson, & E. Palmer. (2000) Autopilot tutor: Building and maintaining autopilot skills. Proceedings of HCI-Aero-2000, International Conference on Htimnn Computer Interaction in Aeronautics. (pages xx - yy) Toulouse, France: Cepadues-Editions.

[23] NTSB (2014) Descent Below Visual Glidepath and Impact With Seawall Asiana Airlines Flight 214 Boeing 777-200ER, HL7742 San Francisco, California July 6, 2013. Accident Report NTSB/AAR-14/01 PB2014-105984

[24] NTSB (2001) Aircraft Accident Report In-Flight Separation of Vertical Stabilizer American Airlines Flight 587 Airbus Industrie A300-605R, N14053 Belle Harbor, New York November 12, 2001.

[25] AAIB (2009) Report on the Serious Incident to Boeing 737-3Q8 , G-THOF on Approach to Runway 26 Bournemouth Airport Hampshire on September 23 2007.

[26] Snowden, D.; M. Boone (2007). A Leader's Framework for Decision Making. Harvard Business Review: 69–76

[27] Lewis, C. Polson, P, Wharton, C. & Rieman, J. (1990) Testing a Walkthrough Methodology for Theory-Based Design of Walk-Up-and-Use Interfaces Chi ’90 Proceedings pp235–242.

Acknowledgements

The authors acknowledge the technical contributions from Immanuel Barshi, Michael Feary, Steve Young (NASA), Julia Trippe (Oregon University), John Shortle, George Donohue, Anvardh Nanduri, Zhenming Wang, Houda Kerkoub , Bahram Yousefi, Michael Hieb (CATSR/GMU) . This research was funded in part by NASA NRA NNX12AP14A and internal funding from the GMU Research Foundation

Email Addresses

lsherry@gmu.edu

rmauro@uo.edu

2015 Integrated Communications Navigation and Surveillance (ICNS) Conference
April 21-23, 2015