Learning from Accidents that are a Consequence of Complex Systems

Dr. John Thomas[1]
Massachusetts Institute of Technology
jthomas4@mit.edu

Captain Shem Malmquist, FRAeS[2]
ISASI MO6149
Member - Resilience Engineering Assoc.
shem.malmquist@gmail.com

Abstract: As the technical and non-technical systems we are building become increasingly complex, the causes of accidents are also becoming more complex. It is becoming more and more difficult to isolate a single or even a few obvious root causes among the abundance of direct and indirect factors that contribute to modern accidents. There is also a growing recognition of the need to better understand human behaviors that contribute to accidents—why might it have made sense at the time for these people to do what they did? Unfortunately, there are few methods to systematically pose and answer these questions and it can be easy to simply treat human error as a conclusion rather than a potential indication of deeper trouble. In addition, the importance of systemic factors, organizational issues, and other high-level factors is widely accepted but there are still few systematic and rigorous methods that can be applied broadly across the entire sociotechnical system including interconnected technical, human, organizational, regulatory, and other issues.

To address these and other issues, a new accident analysis method known as CAST (Causal Analysis using Systems Theory) has been developed at MIT [1]. This methodology provides a comprehensive framework and a step-by-step process to systematically analyze complex accidents, to pinpoint subtle but critical issues like systemic factors that present an "accident waiting to happen", and to identify important unanswered questions that may otherwise be overlooked. In this paper we introduce the CAST methodology as it applies to aircraft accident investigation and demonstrate it with an analysis of the 2014 crash of Asiana B-777 at San Francisco.

[1] Dr. John Thomas is a Research Scientist in MIT's Department of Aeronautics and Astronautics. His research focuses on methods to systematically analyze interactions between hardware, automation, humans, and organizations. He worked in the aerospace industry before joining MIT and he often collaborates with groups from FAA, ATC, NASA, ALPA, airlines, aircraft manufacturers, and others.

[2] Captain Malmquist is currently involved in promoting the concepts of resilience engineering and safety in complex systems, exploring methods to reduce accident rates through both qualitative and quantitative methods and utilizing methods that harness system theory and resilience engineering to predict weaknesses in safety structurers.

Introduction

CAST (Causal Analysis using Systems Theory) is a method to carefully analyze complex accidents and capture a broad array of causes ranging from sharp-end issues (e.g. mechanical and hardware problems, flaws in software and automation design, human behavior) to blunt-end issues like organizational deficiencies, regulatory issues, and other systemic factors. The main objective of CAST is to identify and make sense of the many causes involved in complex accidents, allowing a wide range of potential recommendations and solutions to be identified. CAST does not seek to isolate a few primary causes or identify a single root cause to address. CAST is not about assigning blame. Instead of stopping once unsafe human or component behaviors are identified, CAST provides a framework for analyzing "through" components to explain *why* they did what they did.

Although CAST was developed for accident analysis rather than accident investigation and information gathering, this paper will demonstrate how the process can be applied starting with incomplete information and used to generate questions that can guide the accident investigation. The 2014 crash of Asiana B-777 will be used as a case study to demonstrate the CAST process.

Accident Overview

Asiana Airlines flight 214 struck a seawall during a visual approach to San Francisco International Airport (SFO) on July 6, 2013 [2]. The following events summarize the flight's approach to SFO runway 28:

- ILS is out of service, meaning that a visual approach is needed
- The pilot flying (PF) receives ATC instruction to reduce speed, and does so
- Because the aircraft is in flight level change speed (FLCH SPD) mode, the reduced speed also slows the descent and causes the aircraft to overshoot the glideslope
- PF selects V/S to descend quicker and sets the go around altitude to 3000ft
- PF selects FLCH SPD, which causes the autoflight system to begin a climb toward the previously selected altitude of 3000ft
- The PF immediately disconnects autopilot (A/P) to stop the climb and moves thrust levers to idle
- The new thrust lever position causes the autothrottle (A/T) to automatically switch to HOLD mode, no longer controlling airspeed
- At around 500ft altitude, the aircraft reaches the desired glideslope path and the desired approach speed
- With A/T not controlling the airspeed, the airspeed begins to fall quickly and the aircraft does not stabilize on the desired glideslope path
- At around 100ft, the flight crew initiates a go-around. However, it is initiated 4 seconds too late to avoid a sea wall collision

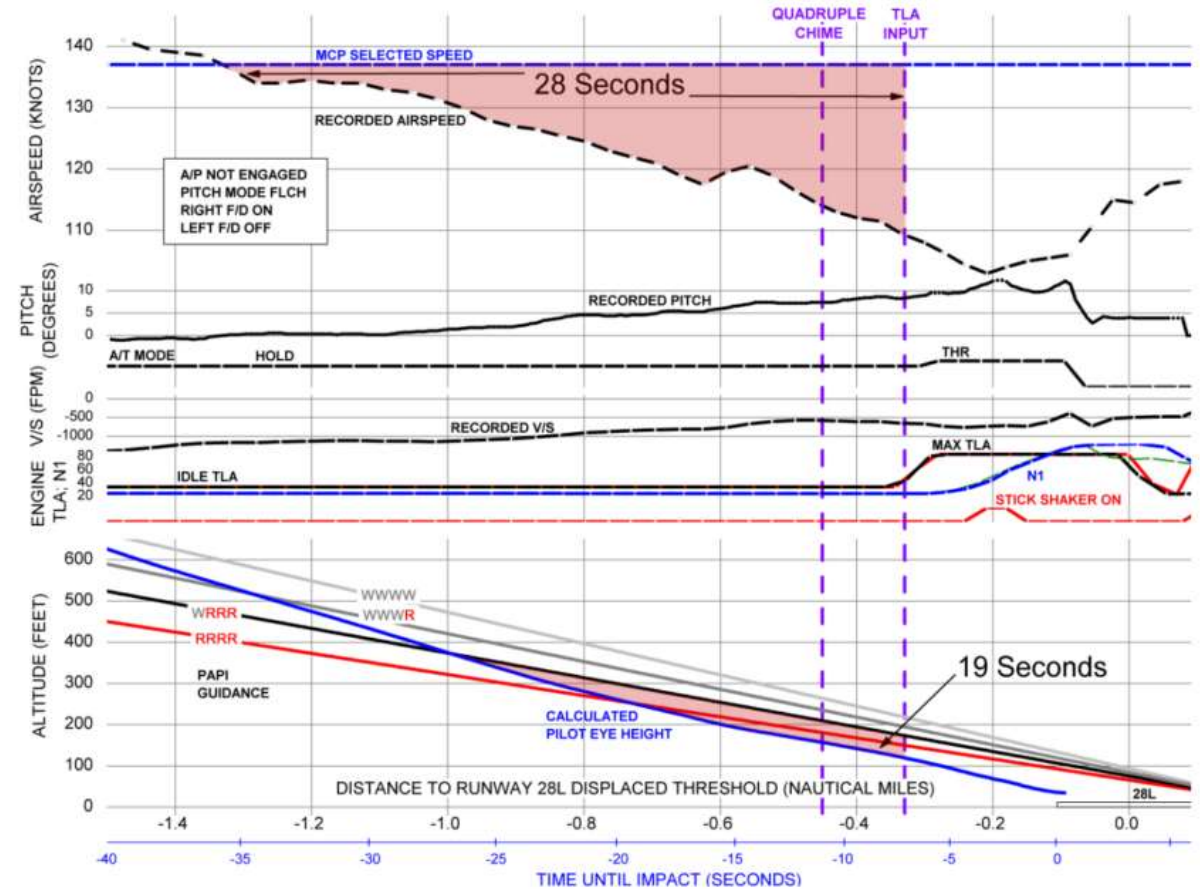

Figure 1: Profile view for the last 40 seconds before impact [2]

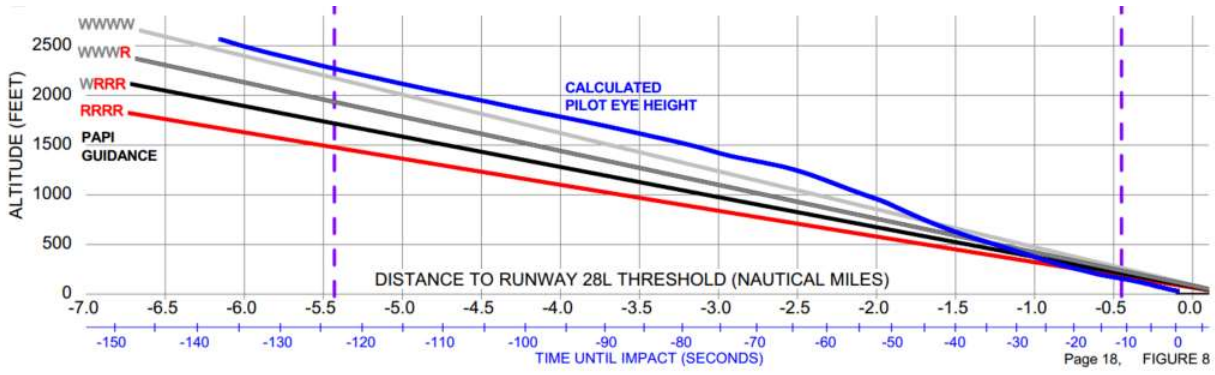

Figure 2: Profile view for the last 2 minutes before impact [2]

Applying CAST

The CAST process consists of the following steps:

1. Identify the System-level Hazard(s) involved in the loss
2. Identify the control structure in place to control the hazard
3. Determine the proximate events leading to the loss

4. Analyze the loss at the physical system level
    a. Identify the physical controls and equipment involved
    b. Identify any physical safety requirements and constraints meant to prevent this accident
    c. Identify any failures or inadequate controls in the physical equipment
    d. Identify contextual factors that explain the physical failures or inadequate controls
5. Analyze higher levels of control to determine how and why each successive higher level contributed to inadequate control at the current level
    a. Identify the safety-related responsibilities for the next higher level of control
    b. Identify the unsafe decisions and control actions
    c. Identify process model flaws (beliefs) that explain the unsafe decisions and control actions
    d. Identify contextual factors that explain why the behavior seemed appropriate at the time

In the case of Asiana 214, the System-level Hazard was uncontrolled flight into terrain.

System-level Hazard:

- SH-1: Uncontrolled flight into terrain

The next step in the CAST process is to develop the control structure in place to control the hazard. The control structure is typically developed iteratively, beginning with a generic or basic control structure as in Figure 3.

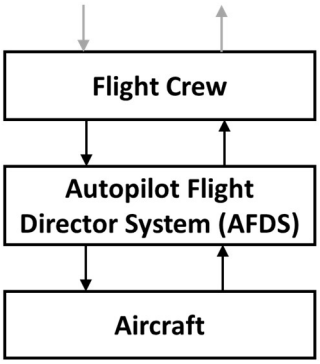

Figure 3: Basic control structure example

The control structure is a model of the hierarchical control in a system. The vertical axis indicates control, meaning that each entity may receive controls or directives from entities that are above it, and it may exert control or authority over entities below it. The lowest entity, in this case the aircraft, typically specifies the physical system that is being controlled. The other entities are controllers that may directly or indirectly control the physical system. The downward arrows indicate controls, commands, or directives that may be exerted while upward arrows indicate information and feedback that may be monitored by controllers and used to make informed decisions.

As the analysis proceeds, the basic control structure is refined. Two types of refinement are possible. The first is to "zoom in", which adds more detail about how the physical system and controllers operate. This refinement provides a better understanding what went wrong and *how* each piece operated. Figure 4 shows how the basic control structure can be refined in this way.

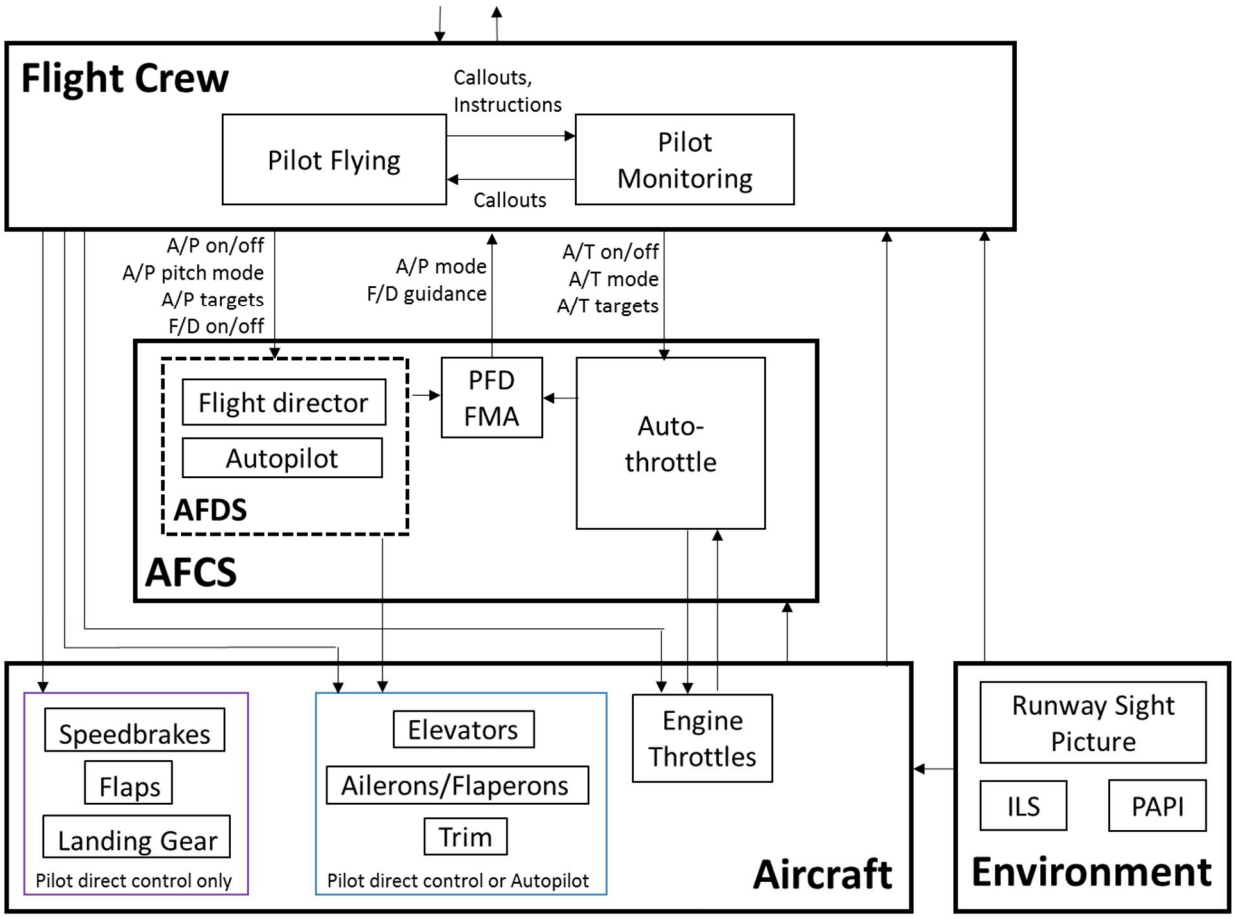

Figure 4: Example of inward control structure refinement for flight crew and AFDS controls

The second type of control structure refinement is to "zoom out"—expanding the boundary to include other elements and controllers. This type of refinement provides a better understanding of *why* the lower-levels operated the way they did. For example, the control structure could be refined to examine higher-level operational controls such as ATC instructions sent to the flight crew, airline SOPs provided to the flight crew, and the design and certification activities by the aircraft manufacturer and authorities. Figure 5 shows an example of this type of refinement.

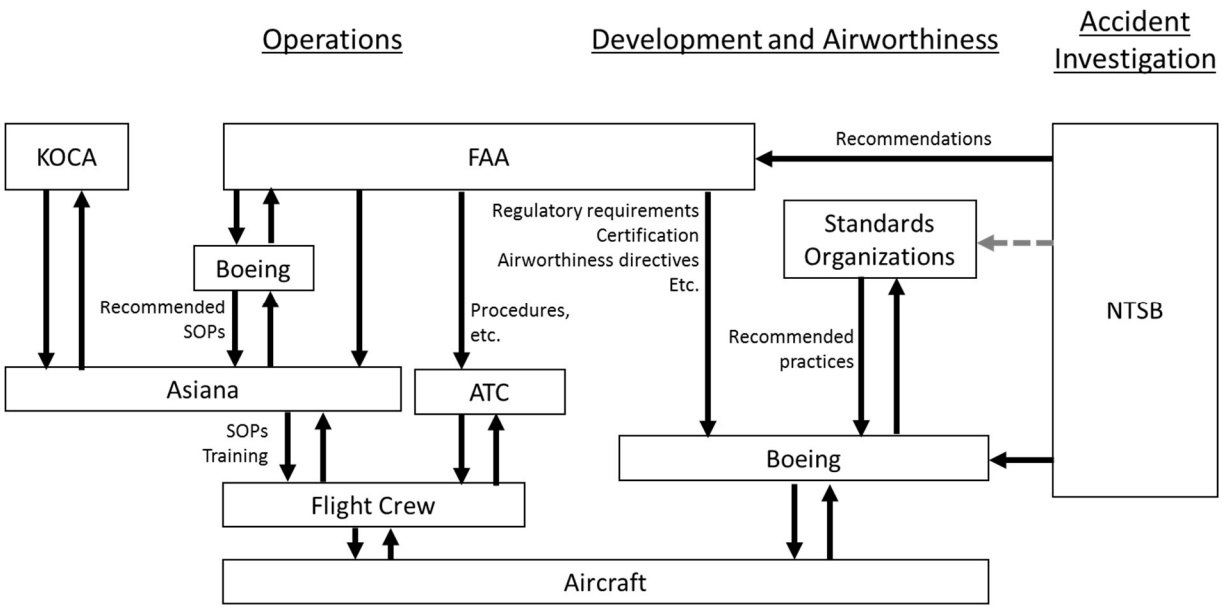

Figure 5: Example of outward control structure refinement to include operations and development activities

In the case of Asiana airlines, the airline is directly regulated by the Republic of Korea Office of Civil Aviation (KOCA) which provides oversight to the airline in a manner similar to the U.S. Federal Aviation Administration (FAA). Asiana is additionally required to obtain a permit issued by the U.S. Department of Transportation and obtain operations specifications issued by the FAA. Operations of foreign air carriers are regulated by FAA under 14 CFR Part 129, which specifies that each air carrier must meet the safety standards contained in International Civil Aviation Organization (ICAO) Annex 6 [2, p.70].

The FAA direct oversight over Asiana under Part 129 is limited to maintaining the operations specifications and oversight as required by the regulations. The FAA can conduct ramp inspections but is not authorized to conduct inspections of operations, nor does FAA approve any of the flight manuals, training programs and the like [2, p.71]. Asiana obtains airplane flight manuals from Boeing, which are in turn vetted through FAA. Asiana then creates its own manuals with approval of KOCA, which also approves the training programs for the airline. Asiana develops the standard operating procedures with oversight from KOCA. Boeing and Asiana would both also be influenced by various organizations that produce recommended standards, and FAA and Boeing will receive recommendations from NTSB. In the case of recommendations, these are not regulatory in nature so may or may not be implemented.

The CAST process can proceed even if the control structure is incomplete. In some cases the relevant controllers and control actions may be immediately obvious, but in other cases they may not be. All that is needed to begin the analysis is an initial control structure. Any of the examples in Figures 3-5 would be sufficient to proceed. If the control structure is initially incomplete, the CAST process will raise questions and identify areas where further refinement is needed.

An initial control structure can usually be identified immediately from the proximal events, as in Figure 4. This paper will demonstrate how the control structure in Figure 4 can be used as a baseline to begin CAST, and we will demonstrate how the process can generate questions and identify areas of further refinement.

Analyzing Physical Systems

Once the control structure and the proximal events have been identified, the next step is to analyze the loss at the physical system level. This is represented by the lowest level in Figure 4. The analysis of the physical system is performed in four parts:

a. Identify physical safety requirements and constraints related to this accident
b. Identify the physical controls and equipment involved
c. Identify any failures or inadequate controls in the physical equipment
d. Identify contextual factors that explain the physical failures or inadequate controls

Figure 6 shows the CAST results for the physical system level. As each part is performed, questions are raised to help guide the analysis. As answers are identified, the next part of the physical analysis is populated and the control structure is refined if needed. For example, PSR-2 refers to the need for glideslope information. What equipment is used to provide glideslope information? PCE-2 and PCE-3 provide the answers, and both link back to PSR-2.

Physical safety requirements and constraints related to this accident

- PSR-1: Aircraft must be controllable along a stable glidepath [SH-1]
- PSR-2: Provide glideslope information to pilots during approach [SH-1]
- PSR-3: Notify controllers when aircraft are on a path to cross a minimum safe altitude [SH-1]
- PSR-4: Warn pilots before a collision with terrain [SH-1]
- PSR-5: Alert pilots when airspeed is below a safe value [SH-1]

Physical controls and equipment to enforce the requirements above

- PCE-1: Engines and control surfaces (elevators, ailerons, etc.) [PSR-1]
- PCE-2: ILS glideslope runway equipment [PSR-2]
- PCE-3: Precision Approach Path Indicator (PAPI) [PSR-2]
- PCE-4: Minimum Safe Altitude Warning (MSAW) system [PSR-3]
- PCE-5: Enhanced Ground Proximity Warning System (EGPWS) [PSR-4]
- PCR-6: Low-speed alert [PSR-5]

Inadequate controls or failures in the physical equipment

- ICF-1: The elevators increased the aircraft pitch during approach, causing a glideslope overshoot [PCE-1]
- ICF-2: The engines stayed at IDLE after intercepting glideslope, did not increase until too late to recover [PCE-1]
- ICF-3: The ILS glideslope was out of service at the time [PCE-2]
- ICF-4: The PAPI operated as designed, and did not warn of a low approach until the aircraft crossed below the desired glideslope about 1 mile / 27 seconds from impact [PCE-3]
- ICF-5: The MSAW operated as configured, and suppressed alerts within 2 miles of SFO [PCE-4]
- ICF-6: The EGPWS operated as designed, but the approach did not meet the criteria to trigger EGPWS alerts [PCE-5]
- ICF-6: The low-speed alert operated as designed, providing the alert 4 seconds too late to recover [PCR-6]

Contextual factors that explain the physical failures or inadequate controls

- CF-1: The elevators received commands from AFDS to increase pitch, causing glideslope overshoot [ICF-1]
- CF-2: The engines received commands from A/T and PF to remain at IDLE, causing a stall [ICF-2]
- CF-3: A construction project required the ILS glideslope to be taken out of service [ICF-3]
- CF-4: The PAPI was only designed to provide instantaneous high/low indications after the aircraft is in visual range [ICF-4]
- CF-5: The MSAW was configured to suppress alerts within 2 miles because the aircraft was expected to be in close proximity to terrain [ICF-5]
- CF-6: The low-speed alert system was calibrated to avoid false positives, and did not take into account low altitude conditions or engine response time.

Figure 6: CAST results for the physical system level

Notice that CAST includes both traditional component failures—defined as components not operating according to their specification—and inadequate controls, including any equipment behavior that was inadequate to prevent the accident. A common pitfall during accident analysis is to relegate oneself to a simple search for component deviations from specified behaviors. This assumes the specified behaviors are correct, appropriate, and safe. CAST does not make this assumption; instead it identifies all unsafe and inadequate behaviors regardless of whether the behaviors were as specified or not. As a result, CAST can help identify a wide range of potential solutions and recommendations including improvements to component specifications and the overall system design.

The last part of the physical analysis identifies contextual factors that explain the inadequate controls or failures. Each contextual factor could serve as a starting point for further analysis or for recommendations. For example, CF-3 explains that a construction project required the ILS glideslope to be taken out of service. This could be analyzed further to examine construction policies and procedures related to ILS, to consider the feasibility of performing construction in a way that does not interrupt ILS or reduces ILS interruptions, to consider the use of portable ILS equipment, etc.

For the purposes of this paper, CF-1 and CF-2 will be explored further. These contextual factors explain that the inadequate physical controls were caused by higher-level controllers. In CAST, the analysis of a human or automated controller is performed in four parts:

a. Identify the controller's safety constraints and responsibilities related to this accident
b. Identify any unsafe control actions or decisions provided by the controller
c. Identify process models (beliefs) that made the control actions seem appropriate at the time
d. Identify contextual factors that explain the unsafe control actions

Figure 7 shows the CAST results for the autothrottle (A/T) controller.

A/T Safety Constraints and Responsibilities

- AT-SCR-1: Automatically manage throttle position when active [SH-1]
- AT-SCR-2: Provide "wake-up" functionality to protect against low airspeed [SH-1]

A/T Unsafe Control Actions or Decisions

- AT-UCA-1: A/T did not wake-up—did not increase throttle to protect against low airspeed [AT-SCR-2]

A/T Process Models

- AT-PM-1: A/T believed it was in HOLD mode and AFDS in FLCH SPD mode [AT-UCA-1]

A/T Contextual factors

- AT-CF-1: A/T was designed to suppress the wake-up functionality in HOLD mode and in FLCH SPD mode [AT-UCA-1]
- AT-CF-2: A/T automatically entered HOLD mode when throttle levers were pulled aft by the PF [AT-UCA-1]
- AT-CF-3: AFDS remained in FLCH SPD mode after the PF disconnected A/P

Figure 7: CAST results for the Autothrottle automation

Unsafe control actions are the actions provided (or not provided) by the controller that led to the accident. As before, this is not limited to deviations from specified behaviors. Even specified behaviors can lead to accidents, as in the case of AT-UCA-1.

Once unsafe control actions are identified, the relevant process models that led to the unsafe control action are identified. The process models represent the controller's beliefs about the world. Accidents are often, but not always, caused when a controller's process model (belief) differs from reality.

Finally, contextual factors that explain the process models and the unsafe control actions are identified. As before, each contextual factor can serve as a starting point for further analysis or recommendations. For example, AT-CF-1 explains that A/T was not designed to "wake-up" in this mode. Further analysis could examine why it was designed this way, and a potential recommendation might be to consider changing the functionality to allow wake-up in this mode.

For the purposes of this paper, AT-CF-2 will be explored further. This contextual factor explains that the HOLD mode was automatically triggered by a higher-level controller: the PF. The CAST analysis of the PF is provided in Figure 8.

PF Safety Constraints and Responsibilities

- PF-SCR-1: Cross check all flight instruments [SH-1]
- PF-SCR-2: Be ready for manual flight before final approach fix [SH-1]
- PF-SCR-3: Maintain stable approach [SH-1]
- PF-SCR-4: Assume manual control and provide safe inputs when needed [SH-1]
- PF-SCR-5: Follow published approach procedures [SH-1]

PF Unsafe Control Actions

- PF-UCA-1: Reduced speed while on glidepath and using FLCH SPD, causing decreased descent rate and glideslope overshoot [PF-SCR-3]
- PF-UCA-2: Selected insufficient descent rate to overcome glidepath overshoot [PF-SCR-3]
- PF-UCA-3: Selected FLCH SPD after final approach fix, causing a climb when aircraft was already above glideslope [PF-SCR-3,4,5]
- PF-UCA-4: Did not announce FLCH SPD when it was selected [PF-SCR-3,5]
- PF-UCA-5: Did not re-engage A/T after it transitioned to HOLD with thrust at idle [PF-SCR-3,5]
- PF-UCA-6: Did not confirm that both flight directors had been turned off as he requested [PF-SCR-1,3,4,5]
- PF-UCA-7: Provided pitch up commands to slow descent with A/T in HOLD, thrust at idle [PF-SCR-3,4]
- PF-UCA-8: Did not initiate a go around when approach was inadequate [PF-SCR-4,5]

PF Process Models

- PF-PM-1: Believed FLCH SPD would facilitate a more rapid descent than V/S mode [PF-UCA-3,1]
- PF-PM-2: Did not know the glidepath had been overshot (initially) [PF-UCA-1,2]
- PF-PM-3: Believed descent rate was sufficient to compensate for glidepath overshoot [PF-UCA-2]
- PF-PM-4: Believed FLCH SPD would not affect A/T [PF-UCA-3,4,5]
- PF-PM-5: Likely believed there was no significant difference between FLCH SPD and V/S, so no need to bother PM in high workload phase [PF-UCA-4]
- PF-PM-6: Believed A/T was still in SPD or THR mode [PF-UCA-4,5,7]
- PF-PM-7: Believed A/T would automatically “wake up” if needed to prevent a stall [PF-UCA-5,7,8]
- PF-PM-8: Believed A/T would always maintain selected airspeed as long at the A/T was on [PF-UCA-5,7,8]
- PF-PM-9: Believed A/T would automatically transition to TO/GA when the aircraft reaches minimum airspeed (as in A320/321) [PF-UCA-5,7,8]
- PF-PM-10: Believed that if a pilot manually overrode the thrust levers and released them, A/T would resume controlling airspeed [PF-UCA-5,7,8]
- PF-PM-11: Believed both flight directors had been turned off [PF-UCA-6]
- PF-PM-12: Before 500ft, believed the approach could be salvaged. At 500ft, believed the aircraft was on the desired approach glidepath [PF-UCA-8]
- PF-PM-13: Believed the policy was to stabilize the approach by 300ft or go around (not 500ft) [PF-UCA-8]
- PF-PM-14: Believed that only the PM (PIC) had authority to decide to go-around, due to previous tailstrike that occurred after a go around was initiated [PF-UCA-8]
- PF-PM-15: Believed the instructor pilot was monitoring his actions, and would catch mistakes and intervene if necessary [PF-UCA-1,2,6,7,8]

PF Contextual factors

- PF-CF-1: The PF was new to the 777 and still learning, having only 33 hours of 777 flight time [PF-UCA-3,4,5,7,8]
- PF-CF-2: This was the first time the PM was acting as an instructor pilot. There was no requirement to ensure new 777 pilots are monitored by an experienced instructor pilot [PF-UCA-4,5,8]
- PF-CF-3: The 777 A/T behavior had confused even the more experienced Asiana 777 instructors [PF-UCA-5,7,8]
    - When other Asiana 777 instructor captains were asked about the A/T mode change when thrust levers are pulled back, only 2 out of 4 captains knew it would transition to HOLD mode.
    - When other Asiana 777 instructors and training captains were asked about A/T low speed protection, 3 out of 5 said they were previously unaware that low speed protection is not provided in HOLD mode
- PF-CF-4: The PF's 777 training regarding A/T behavior was inadequate [PF-UCA-3,5,7]
    - The PF's 777 simulator training demonstrated the A/T "wake up" feature that provides low speed protection, but did not demonstrate that the feature doesn't work with A/T in HOLD mode
    - Manual flying training that included the approximate power settings and pitch attitudes required to achieve the glidepath was not in the training syllabus
    - A training module on the B777 flight controls incorrectly stated that the stall protection feature automatically engages the autothrottle if it is armed
    - The above training modules did not specify that A/T would not activate when A/T is in HOLD mode
- PF-CF-5: The manuals contained conflicting information about the responsibilities and authority for go-around decisions [PF-UCA-8]
    - Asiana 777 Pilot Operation Manual 2.13.6.8 specifies that the PM should call out "five hundred" at 500ft, and the PF should respond with a "stabilized" or "go-around" decision
    - Asiana 777 Pilot Operation Manual 2.19.1.1 specifies that the decision to make a missed approach rests with the captain.
- PF-CF-5: All of the 777 approaches the PF had previously flown during OE were ILS approaches. There was no requirement to perform visual approaches during OE [PF-UCA-3,4,5,7]
- PF-CF-6: Pilots avoided flying manually because of concern that the company would blame them if they performed a go around or had a bad approach/landing that was captured by onboard flight data monitoring devices [PF-UCA-7]
- PF-CF-7: No clear intuitive indication of aircraft position with respect to glideslope, or that the glideslope had been overshot (initially) – although a "green arc" would have been available on the Navigation Display (ND), on a high workload visual approach it is outside the normal pilot scan area [PF-UCA-1,2]
- PF-CF-8: The approach was almost salvaged as the aircraft approached 500ft. The aircraft was on the glideslope, the airspeed was within the desired range, and the PAPI showed two white and two red lights indicating a good glidepath. [PF-UCA-8]
- PF-CF-9: Most pilots (96%) don't initiate go around even when approach is not stable [3]. [PF-UCA-8]
- PF-CF-10: The PF was transitioning from the A320, where low speed protection (alpha floor protection) would have been available [PF-UCA-5,7,8]
- PF-CF-11: The unintuitive behavior of FLCH SPD mode and A/T engagement was previously reported by the FAA's primary project pilot [PF-UCA-5,7]
- PF-CF-12: The PF was concerned about failing his OE training flight [PF-UCA-8]

- PF-CF-13: The PF may not have considered the deference a new instructor would give to a seasoned student who had been a check airman and instructor on another fleet for a time far longer than the new instructor, creating more conflict of roles. [PF-PM-15]

Figure 8: CAST results for the PF

The PF clearly provided a number of unsafe control actions, but CAST does not stop once human unsafe control actions or human errors are identified. As human factors experts have noted, human error is not a root cause of accidents but rather a symptom of deeper trouble in the system [4]. CAST provides a framework to understand why the humans behaved the way they did and identify the deeper systemic trouble.

For example, the PF contextual factors explain that the A/T behavior and the loss of airspeed protection was confusing to many other more experienced pilots, that the Asiana training was inadequate, the Asiana manuals included conflicting information about go-around decisions, and that the training. As before, each of these contextual factors provides a starting point for recommendations and further analysis.

Figure 9 shows the CAST results for Asiana.

Asiana Safety Constraints and Responsibilities

- A-SCR-1: Provide pilot training and testing [SH-1]
- A-SCR-2: Provide standard operating procedures [SH-1]
- A-SCR-3: Provide policies for scheduling OE training flights [SH-1]

Asiana Unsafe Control Actions or Decisions

- A-UCA-1: Provided inadequate training regarding A/T behavior [A-SCR-1]
- A-UCA-2: Provided operating procedures and manuals with conflicting information about go-around decisions [A-SCR-2]
- A-UCA-3: Matched a new trainee pilot with a new instructor pilot [A-SCR-3]
- A-UCA-4: Had no requirement for visual approaches during OE flights [A-SCR-1,2]
- A-UCA-5: Recommended full use of automation whenever possible (impacts manual flying proficiency) [A-SCR-2]
- A-UCA-6: Provided no training for achieving the appropriate glidepath with manual flying[3] [A-SCR-1]
- A-UCA-7: Blamed pilots for go-arounds or hard landings based on flight data, creating a fear of flying manually[4] [A-SCR-1]
- A-UCA-8: Did not enforce stabilized approach criteria for go arounds [A-SCR-1,2]
- A-UCA-9: Recommended not to use FLCH SPD after FAF, but did not ensure that pilots understood why [A-SCR-1,2]
- A-UCA-10: Recommended turning of both F/Ds and then turning PM F/D back on, but did not ensure that pilots understood why [A-SCR-1,2]
- A-UCA-11: Provided standard callout procedures, but did not ensure pilots actually followed them [A-SCR-1,2]

Asiana Process Models

- A-PM-1: Believed the training for A/T behavior was adequate, had no mechanism to detect the deficiencies [A-UCA-1]
- A-PM-2: Believed there were no conflicts in the operating procedures and manuals, had no mechanism to detect the deficiencies [A-UCA-2]
- A-PM-3: Believed the use of full automation whenever possible would improve overall safety [A-UCA-5]
- A-PM-4: Believed that blaming pilots for flight anomalies would improve overall safety [A-UCA-7]
- A-PM-5: May have believed the stabilized approach criteria was being followed [A-UCA-8]
- A-PM-6: May have believed pilots were following standard callouts [A-UCA-11]

Asiana Contextual factors

- A-CF-1: Asiana training and procedures were based on materials provided by Boeing (A-UCA-1,2,6]
- A-CF-2: Had no mechanism to detect deficiencies in training and procedures [UCA-1,2,4]
- A-CF-3: Go arounds are costly for the airline, creating an incentive to stabilize approaches when possible [A-UCA-7]

Figure 9: CAST results for Asiana

[3] "Asiana contract simulator instructor … stated that manual flying training that included the approximate power settings and pitch attitudes required to achieve a 3° glidepath was not in the training syllabus." [2, p.63]

[4] "An Asiana contract simulator instructor stated that manual flying was a "big scare for everybody," and he believed that pilots avoided flying manually because of concern that they might do something wrong and the company would blame them if they performed a go-around or had a hard landing that was captured by onboard flight data monitoring devices." [2, p.63]

Although a number of inadequacies existed at Asiana, the CAST analysis again helps identify deeper issues that existed. For example, some of the inadequate training materials used by Asiana were provided to Asiana by Boeing.

Figure 10 shows the CAST results for Boeing.

Boeing Safety Constraints and Responsibilities

- B-SCR-1: Provide aircraft that can be operated safely [SH-1]
- B-SCR-2: Perform risk assessment and hazard analysis, and address safety issues [SH-1]
- B-SCR-3: Provide recommended standard operating procedures to airlines [SH-1]
- B-SCR-4: Provide pilot training materials [SH-1]
- B-SCR-5: Modify aircraft, recommended procedures, and training materials when safety issues are discovered [SH-1]

Boeing Unsafe Control Actions or Decisions

- B-UCA-1: Created A/T automation with confusing behavior that automatically enters HOLD mode in certain conditions and automatically disables low-speed protection in HOLD mode [B-SCR-1,2]
- B-UCA-2: Did not provide a low energy alert that takes into account low altitude or engine response time [B-SCR-1,2]
- B-UCA-3: Did not provide a clear indication of when A/T low speed protection was available [B-SCR-1,2]
- B-UCA-4: Did not provide a clear indication of vertical position relative to the glideslope, or whether the glideslope had been overshot [B-SCR-1,2]
- B-UCA-5: Provided operating procedures and materials to Asiana with incorrect or no information about when low speed protection is unavailable [B-SCR-4]
- B-UCA-6: Did not make any significant changes to the 777 aircraft, recommended procedures, or training materials after receiving reports of unsafe A/T behavior from pilots, airlines, and regulatory agencies.

Boeing Process Models

- B-PM-1: Believed the training for A/T behavior was adequate, had no mechanism to detect the deficiencies [A-UCA-1]
- B-PM-2: Believed there were no conflicts in the operating procedures and manuals, had no mechanism to detect the deficiencies [A-UCA-2]

Boeing Contextual factors

- B-CF-1: The unintuitive behavior of FLCH SPD mode and A/T engagement was previously reported by the FAA's primary project pilot [B-UCA-1]
- B-CF-2: As a result of B-CF-1, the FAA required Boeing to add a note about unintuitive A/T behavior in the 787 Flight Manual. Although the 777 used identical A/T automation, Boeing did not update the 777 manual because it had been previously approved by the FAA [B-UCA-1,6]
- B-CF-3: The 777 A/T behavior had confused even experienced 777 instructors [B-UCA-1]
    - When other Asiana 777 instructor captains were asked about the A/T mode change when thrust levers are pulled back, only 2 out of 4 captains knew it would transition to HOLD mode.
    - When other Asiana 777 instructors and training captains were asked about A/T low speed protection, 3 out of 5 said they were previously unaware that low speed protection is not provided in HOLD mode
- B-CF-4: EASA published concern about the A/T engagement in May 2011, recommending changes to the A/T behavior. "Although the certification team accepts that this Autothrottle wake up feature is not required per certification requirements, these two exceptions look from a

pilot's perspective as an inconsistency … an item which meets the required standard but where considerable improvement is recommended." [B-UCA-1]

- B-CF-5: A low airspeed alert was provided, but it was calibrated to avoid false positives and did not take into account low altitude or engine response time. It sounded 4 seconds too late for the crew to respond and recover. It was implemented as a general caution chime, which can signify more than 60 other problems on the 777 and requires more time for crew to respond compared to warnings. [B-UCA-2]
- B-CF-6: After a B737 crash in Schiphol in 2009, the DSB previously asked Boeing to implement a verbal low-speed warning to allow faster crew response in emergencies. Boeing made the change to B737 aircraft, but not B777 aircraft. [B-UCA-2]
- B-CF-7: The 777 flight crew operating manual was updated in 2012, relocating a discussion of A/T's automatic activation feature to a different section [B-UCA-6]
- B-CF-8: The FAA issued a policy in 2009 in response to four accidents, specifying that it intends to ensure "a speed protection function for all operation modes". The B777 did not provide a speed protection in HOLD mode. [B-UCA-1]
- B-CF-9: Boeing had followed all applicable certification standards and processes, but there are gaps in the standards and processes used. For example, 14 CFR 25.1329 requires that the flight guidance system "must be designed to minimize flightcrew errors and confusion concerning the behavior and operation of the flight guidance system" [5]. This requirement did not exist prior to 2006 when the autothrottle system was originally certified, and the new requirement was not applied retroactively. However, these autothrottle confusion issues would still be overlooked today even with the new requirement. The FAA's Advisory Circular 25.1329 [6]—which describes an acceptable means to show compliance with 14 CFR 25.1329—specifies generic criteria like "indications must be grouped and presented in a logical and consistent manner" and would not have prevented the autothrottle issues described above.
- B-CF-10: Significant changes would be costly, especially changes to the aircraft [B-UCA-6]

Figure 10: CAST results for Boeing

Generating Recommendations

Once the CAST analysis has been performed, recommendations can be generated from the analysis. Each issue identified in the analysis is a candidate for corrective action. At least three categories of recommendations can be identified:

- Recommendations related to the actual aircraft and equipment
- Recommendations related to operating procedures, policies, and training
- Recommendations related to development processes

Figure 11 Shows the recommendations generated from the CAST results so far. Every recommendation is traceable to one or more factors in the CAST analysis that it would address. This traceability makes it easy to determine what gaps may exist in the set of recommendations and what causal factors have not been addressed. It is also possible to prioritize the recommendations based on the number of issues it would address, the cost to implement the recommendation, etc.

Recommendations related to aircraft and equipment (Boeing and FAA)

R-1: Consider feasibility of configuring existing equipment to detect and warn about this type of accident (MSAW, EGPWS, low airspeed alerts, etc.) [ICF-5,6; B-CF-5]

R-2: Consider providing low energy warnings that take into account low altitudes and engine response time [B-UCA-2; B-CF-5]

R-3: Consider allowing A/T to provide wake-up functionality in HOLD and/or FLCH SPD mode [AT-UCA-1; AT-CF-1; PF-CF-3,11; B-UCA-1]

R-4: Consider providing a clear indication of when A/T low speed protection is available [B-UCA-3]

R-4: Consider designing A/T so it doesn't automatically transition to HOLD mode when throttle levers move aft in FLCH SPD mode [AT-CF-2; PF-CF-3,11; B-UCA-1]
R-5: Consider designing A/T so the automatic transition to HOLD mode is consistent with other A/T and AFDS-pitch modes [AT-CF-2; PF-CF-3; B-UCA-1]
R-6: Consider a more intuitive and robust way to reset AFDS mode with A/P disconnected (other than manually turning both F/Ds off momentarily and then turning one on again) [AT-CF-3; PF-UCA-6; PF-PM-11]
R-7: Consider potential automated callouts rather than relying on human callouts [PF-UCA-4,6; PF-PM-4,6,11]
R-8: Consider mechanism for monitoring stabilized approach criteria, providing reliable indication of when go around is warranted [PF-UCA-8; PF-PM-12,13,14]

Potential improvements to procedures, policies, and training (Asiana and Boeing)

R-9: Determine why callouts are commonly being ignored, and adjust the callout procedures accordingly [PF-UCA-4,8; PF-PM-11; A-UCA-11; A-PM-6]
R-10: Consider ways to verify or confirm that callouts are being announced [PF-UCA-4,8; PF-PM-11; A-UCA-11; A-PM-6]
R-11: Provide a clear and consistent definition of go around responsibilities. Specify who makes go around decisions, when, and how. Confirm that these responsibilities and procedures are being followed. [PF-UCA-8; PF-PM-12,13,14; PF-CF-5,9; A-UCA-2,8; A-PM-5]
R-12: Indicate in the procedure why the F/D should be turned off and then on again [PF-UCA-6; PF-PM-11; A-UCA-10]
R-13: Provide procedures and training for capturing/maintaining the glideslope on visual approach, including recovering from an overshoot [PF-UCA-1,2,3; A-UCA-6]
R-14: Require manual flying training that includes power and pitch settings to achieve the glideslope [A-UCA-6]
R-15: Require that new transition pilots are matched with experienced instructor pilots [PF-CF-1,2; A-UCA-3]
R-16: Require that training includes the limitations in the A/T wakeup feature, low speed protection, and automatic mode changes [PF-CF-4; A-UCA-1]
R-17: Consider requiring visual approaches as part of OE training [PF-CF-5; A-UCA-4]
R-18: Consider encouraging more manual flying to maintain proficiency. This includes not blaming the pilots for go arounds or hard landings based on flight data monitoring. [PF-CF-6; A-UCA-5,7; A-PM-3,4]
R-19: Ensure that procedures and training explain why FLCH SPD should not be used after FAF [A-UCA-9]
R-20: Create a mechanism to discover and address deficiencies in training, procedures, and manuals, like the missing and conflicting information about A/T wake-up and mode changes [A-PM-1,2]
R-21: Consider ways to verify or confirm that the stabilized approach criteria are followed [A-UCA-8; A-PM-5]
R-22: Identify and eliminate conflicts or perceived conflicts that encourage pilots to follow through with unstable approaches [A-UCA-7; A-CF-3]
R-23: Create policies and procedures to ensure reports of unintuitive or potentially dangerous behaviors are reviewed and that procedures and training materials are revised. [B-UCA-6; B-CF-1,2,3,4]
R-24: Create policies and procedures to ensure that when procedures and training materials are fixed or updated for one aircraft, the procedures and materials for other aircraft with identical automation are also fixed or updated. [B-UCA-6; B-CF-2]

Recommendations related to aircraft development and certification processes (Boeing and FAA)

R-25: Identify the gaps in engineering development and certification processes that overlooked poor design decisions, and update the processes to catch these issues before operation. [B-CF-9]

Figure 11: Recommendations generated from the CAST analysis

The CAST analysis identified 94 causal factors that contributed to this accident, ranging from technical design issues to human factors issues and organizational deficiencies. 25 recommendations were generated, ranging from technical to procedural and development issues.

Comparison of CAST and NTSB Recommendations

Although the CAST analysis was performed using the same factual data set as the NTSB analysis, there are some notable differences in the recommendations produced. First, the CAST analysis intentionally focused only on the causes of the crash for the purposes of demonstrating the concepts of CAST, and so many aspects were not analyzed including survival factors like the rescue response and passenger seatbelt use. The NTSB analysis produced 27 recommendations, 14 of which involved the accident response after the crash and were considered out-of-scope for the purposes of this CAST project. The 13 NTSB recommendations that addressed causes of the crash are shown in Figure 12.

To the Federal Aviation Administration:

- Require Boeing to develop enhanced 777 training that will improve flight crew understanding of autothrottle modes and automatic activation system logic through improved documentation, courseware, and instructor training.
- Once the enhanced Boeing 777 training has been developed, as requested in Safety Recommendation A-14-37, require operators and training providers to provide this training to 777 pilots.
- Require Boeing to revise its 777 Flight Crew Training Manual stall protection demonstration to include an explanation and demonstration of the circumstances in which the autothrottle does not provide low speed protection.
- Once the revision to the Boeing 777 Flight Crew Training Manual has been completed, as requested in Safety Recommendation A-14-39, require operators and training providers to incorporate the revised stall protection demonstration in their training.
- Convene an expert panel (including members with expertise in human factors, training, and flight operations) to evaluate methods for training flight crews to understand the functionality of automated systems for flightpath management, identify the most effective training methods, and revise training guidance for operators in this area.
- Convene a special certification design review of how the Boeing 777 automatic flight control system controls airspeed and use the results of that evaluation to develop guidance that will help manufacturers improve the intuitiveness of existing and future interfaces between flight crews and autoflight systems.
- Task a panel of human factors, aviation operations, and aircraft design specialists, such as the Avionics Systems Harmonization Working Group, to develop design requirements for context-dependent low energy alerting systems for airplanes engaged in commercial operations.

To Asiana Airlines:

- Reinforce, through your pilot training programs, flight crew adherence to standard operating procedures involving making inputs to the operation of autoflight system controls on the Boeing 777 mode control panel and the performance of related callouts.
- Revise your flight instructor operating experience (OE) qualification criteria to ensure that all instructor candidates are supervised and observed by a more experienced instructor during OE or line training until the new instructor demonstrates proficiency in the instructor role.
- Issue guidance in the Boeing 777 Pilot Operating Manual that after disconnecting the autopilot on a visual approach, if flight director guidance is not being followed, both flight director switches should be turned off.
- Modify your automation policy to provide for more manual flight, both in training and in line operations, to improve pilot proficiency.

To Boeing:

- Revise the Boeing 777 Flight Crew Operating Manual to include a specific statement that when the autopilot is off and both flight director switches are turned off, the autothrottle mode goes to speed (SPD) mode and maintains the mode control panel-selected speed.
- Using the guidance developed by the low energy alerting system panel created in accordance with Safety Recommendation A-14-43, develop and evaluate a modification to Boeing wide-body automatic flight control systems to help ensure that the aircraft energy state remains at or above the minimum desired energy condition during any portion of the flight.

Figure 12: NTSB recommendations to address causes of the crash

Some of the CAST and NTSB recommendations are identical, such as the recommendation to provide more manual flight experience to improve proficiency. Other recommendations are similar but not identical, such as the recommendation for more experienced instructors.

Two of the NTSB recommendations involve convening a panel of experts to identify solutions; these recommendations do not appear in the CAST recommendation list. The other NTSB recommendations all overlap with corresponding CAST recommendations.

Almost all of the CAST recommendations involving the aircraft and equipment do not appear in the NTSB recommendation list, perhaps because of the perceived cost of making changes to the aircraft. The exception was the low energy alerting system, which was recommended by both analyses.

Other CAST recommendations that do not appear in the NTSB recommendation list include identifying why callouts are routinely being ignored, addressing inconsistencies in the go around responsibilities, requiring visual approaching during OE training, developing mechanisms to discover gaps in training, etc.

Perhaps the most important CAST recommendation is R-25, which refers to gaps in the overall aircraft development and certification process. After all, why wasn't this accident anticipated when the autothrottle automation was originally designed? Unfortunately the current aircraft development and certification standards seem to overlook this type of problem.

Discussion and Conclusions

Although a careful team of very experienced and qualified experts may identify some or even all of these issues without CAST, accident analysis should not rely solely on the hope that sufficient expertise will be found within the investigation team. Another challenge is that even teams of experienced experts will be susceptible to human biases and can be lead down the wrong path. CAST provides a systematic methodology to guide even less experienced teams and ensure a systematic and repeatable analysis is performed.

In this case, the expertise of the NTSB and the major investigation staff was clearly highlighted in the comprehensiveness of the Asiana report. Again, though, this is due to the fact that the level of expertise available to the NTSB can be quite good especially for high-profile accidents. While perhaps not a factor at NTSB, there are times, depending on the investigative agency, when staff or technical advisors' recommendations do not make it into the final report or findings due to the biases of those at high levels in the organization who must approve the final report. If there are recommendations from the staff that did not get included, then utilizing a standardized CAST methodology would help ensure that relevant factors are always included. It would also help ensure that comprehensive recommendations are elicited more consistently even when a world class team is not available or possible, or when political pressures or hierarchy within an agency led to factors not being included. The use of CAST would create a "paper trail" that might mitigate these issues.

The CAST process maintains traceability between every result. Every recommendation is traceable to one or more causal factors, which are linked to unsafe control actions or inadequate controls, to the safety requirements, and finally to the system-level hazard. This traceability makes it easy to review the analysis, collaborate on the analysis in parallel teams, identify the source of every result and where it came from, and minimize the subjectivity in the findings and recommendations.

Although this paper demonstrated CAST applied to Asiana 214, many of the CAST results are not unique to this accident. For example, the control structures, the physical safety requirements, and the physical equipment that enforce the requirements all reflect standard designs and decisions and could easily be re-used in other accidents. The inadequate controls and the specific unsafe control actions could be unique especially at lower levels of the control structure, but they are often remarkably similar at higher levels.

The CAST process provides a standard way to organize many factors involved in an accident, and this framework could be used to systematically compare similar types of contributing factors across many accidents. Such a comparison could identify the most common unsafe control actions, process model

flaws, etc. that lead to aviation accidents in general, and can potentially provide more insight than comparing arbitrary root causes.

Although CAST focuses on learning as much as possible from past accidents, it is also important to anticipate and prevent future accidents. System Theoretic Process Analysis (STPA) [1] is a method that uses the same framework as CAST to anticipate accidents before they happen. STPA uses the same control structure model, but includes additional guidance to anticipate unsafe control actions and accident scenarios. Ideally, methods like STPA would be applied during development to anticipate and prevent these kinds of accidents rather than relying only on reactionary accident analysis. The gaps in current certification standards and processes, like the one described in B-CF-9 in Figure 10, can be addressed with new methods like STPA.

As methods improve and our understanding of human factors and complex systems evolves it has become clear that many previous accident reports contain incorrect, misleading or incomplete findings. Despite this fact, these findings are often used as a basis for subsequent research and recommendations which may skew our understanding of human response, common accident causes, and the appropriate lessons learned. Unlike scientific literature, which when an error is found it is corrected and revised in newer research, or sometimes withdrawn completely, official accident reports remain part of database drawn from for researchers and are only very rarely corrected or revised. Therefore it is important to ensure high-quality accident analysis and investigation is always performed, and systematic methods like CAST are an important step in that direction.

References

[1] Leveson, N., *Engineering a safer world: systems thinking applied to safety*. Engineering systems. 2012, Cambridge, Mass.: MIT Press. xx, 534 p.

[2] National Transportation Safety Board. *Descent Below Visual Glidepath and Impact With Seawall, Asiana Airlines Flight 214, Boeing 777-200ER, HL7742, San Francisco, California, July 6, 2013*. June 24, 2014.

[3] Blajev, T., Curtis, W. *Final Report to Flight Safety Foundation: Go-Around Decision-Making and Execution Project.* Flight Safety Foundation. March 2017, available at https://flightsafety.org/wp-content/uploads/2017/03/Go-around-study_final.pdf

[4] Dekker, S. *The Field Guide to Understanding Human Error.* CRC Press, 2017

[5] Electronic Code of Federal Regulations. *Title 14, 25.1329: Flight guidance systems*. U.S. Government Publishing Office. Doc No. FAA-2004-18775, 71 FR 18191, Apr 11, 2006

[6] Federal Aviation Administration. *Approval of Flight Guidance Systems.* Advisory Circular 25.1329-1C. May 24, 2016