Captain Shem Malmquist
Visiting Professor, Florida Institute of Technology
274 E. Eau Gallie Blvd. 252, Indian Harbour Beach, FL 32937
smalmquist2012@fit.edu

Captain Shem Malmquist is a visiting professor at the Florida Institute of Technology, an experienced accident investigator and an active current B-777 Captain. His work includes Automation and Human Factors lead for the Commercial Aviation Safety Team's Joint Safety Implementation Team, Loss of Control working group, the Aircraft State Awareness working group and the Joint Implementation Measurement and Data Analysis Team. He is an elected Fellow of the Royal Aeronautical Society, a full member of ISASI, REA, AIAA, HFES, IEEE, FSF and SAE's Flight Deck and Handling Quality Standards for Transport Aircraft working group.

Prof. Nancy Leveson
Aeronautics and Astronautics
MIT, Room 33-334
77 Massachusetts Ave.
Cambridge, MA 02142

Telephone: 617-258-0505 (MIT)
Mobile: 617-460-5749

Email: leveson@mit.edu
URL: http://sunnyday.mit.edu

Dr. Nancy Leveson is a professor of Aeronautics and Astronautics at MIT. She has worked in system safety engineering for over 35 years. One common element in her work is an emphasis on applying systems thinking to complex systems and integrating humans and social systems with engineering considerations. She consults extensively on the ways to prevent accidents and has served on numerous national and international committees and accident investigations. She was an expert consultant for the Columbia Space Shuttle Accident Investigation Board, the Presidential Commission on Deepwater Horizon, the Baker Panel on the Texas City oil refinery explosion, and other lesser known losses.

==

Investigating Accidents in Highly Automated Systems: Systemic Problems Identified Through Analysis of Air France 447

Shem Malmquist[1], Nancy Leveson[2]

Introduction

Most accident analyses are based on *ad hoc* approaches. Many formal analysis techniques have been proposed, but few are widely used. This case study shows how a structured process called CAST (Causal Analysis based on Systems Theory), based on a more powerful model of accident causation, can improve the results of accident investigation. The case study used is aerodynamic stall accident involving an Air France flight 447, an Airbus A330 aircraft while cruising at an altitude of 35,000 feet on a flight from Rio de Janeiro, Brazil, to Paris, France on June 1st, 2009. The results are compared with the official BEA accident report. The BEA did an exceptionally good job on this accident and the BEA is considered one of the foremost top tier accident investigation agencies on the world. Therefore, a comparison of the results is informative about how accident investigation and analysis might be improved beyond the standard approach used by the BEA and most others.

The structured analysis method used, called CAST[3] (Causal Analysis based on System Theory), is based on an expanded accident model called STAMP (Systems-Theoretic Accident Model and Processes) [Leveson, 2012]. Traditionally, accidents have been thought of as resulting from a chain of failure events, each event directly related to the event that precedes it in the chain. For example, the baggage door is not completely closed, the aircraft climbs to a level where unequal pressure between the cargo compartment and the passenger cabin causes the cabin floor to collapse, the cables to the control surfaces (which run through the floor) are severed, the pilots cannot control the aircraft, and the plane crashes. The biggest problem with such a chain-of-events model is what it omits. For example, why did the design of the baggage door closure mechanism made it difficult to determine whether it was effectively sealed? Why did the pilots not detect that the door was not shut correctly? Why did the engineers create a design with a single point failure mode by running all the cables through the cabin floor? Why did the FAA certification process allow such designs to be used? And so on. While these additional factors can be included in accident investigation and analysis, there is no structured process for making sure that “systemic” causal factors are not missed.

STAMP extends the traditional model of accident causation to include the chain-of-events model as one subcase but includes the causes of accidents that do not fit within this model, particularly those that occur in the complex sociotechnical systems common today. These causes (in addition to component failure) include system design errors, unintended and unplanned interactions among system components (none of which may have failed), flawed

[1] Florida Institute of Technology
[2] Aeronautics and Astronautics Dept., MIT
[3] Unfortunately, the acronym CAST for this accident analysis approach has an important conflict in the aviation community. CAST has been used as an accident analysis technique for close to 20 years in the safety community and for about the same time in aviation to denote Commercial Aviation Safety Team, without either group being aware of the conflict. In this paper, CAST appears only as a reference to the accident analysis technique

safety culture and human decision making, inadequate controls and oversight, and flawed organizational design. In STAMP, accidents are treated as more complex processes than simple chains of failure events. The focus is not simply on the events that led to the accident, but ***why*** those events occurred.

The other significant difference is that, instead of focusing on failures, STAMP assumes that accidents are caused by a lack of effective enforcement of safety constraints on the system behavior to prevent hazardous states or conditions. Thus, safety becomes a control problem, not a failure problem. Controls are created to prevent hazards, such as a stall. Such controls clearly include pilot knowledge, but they also include the aircraft envelope protection system, the aircraft warning systems, pilot training, standards, government regulation and oversight, etc. Theoretically, the extensive controls that have been introduced to eliminate stalls should have prevented the accident. Why didn't they? How can we learn from the accident to improve those controls?

Because individual controls and controllers may not be adequate or effective, there are almost always many types of controls used. The goal of accident analysis should be not to identify someone to blame (in practice this is usually the flight crew) because they did not satisfy their particular role in preventing a hazard such as a stall but to identify all the flaws in the safety controls that allowed the events to occur, to understand why each of these controls was not effective, and to learn how to strengthen the controls and the design of the safety control system in general to prevent similar losses from occurring in the future.

In this paper, CAST is demonstrated with a case study of a stall accident of Air France 447. The official BEA accident report (BEA, 2012) summarizes the accident (the chain of events) in the following way:

> On Sunday 31 May 2009, the Airbus A330-203 registered F-GZCP operated by Air France was programmed to perform scheduled flight AF 447 between Rio de Janeiro Galeão and Paris Charles de Gaulle. Twelve crew members (3 flight crew, 9 cabin crew) and 216 passengers were on board. The departure was planned for 22 h 00.
>
> At around 22 h 10, the crew was cleared to start up engines and leave the stand. Takeoff took place at 22 h 29. The Captain was Pilot Not Flying (PNF); one of the copilots was Pilot Flying (PF).
>
> At the start of the Cockpit Voice Recorder (CVR) recording, shortly after midnight, the aeroplane was in cruise at flight level 350. Autopilot 2 and auto-thrust were engaged. Auto fuel transfer in the "trim tank" was carried out during the climb. The flight was calm.
>
> At 1 h 35, the aeroplane arrived at INTOL point and the crew left the Recife frequency to change to HF communication with the Atlántico Oceanic control centre. A SELCAL test was successfully carried out, but attempts to establish an ADS-C connection with DAKAR Oceanic failed.
>
> Shortly afterwards, the co-pilot modified the scale on his Navigation Display (ND) from 320 NM to 160 NM and noted *"…a thing straight ahead"*. The Captain confirmed and the crew again discussed the fact that the high temperature meant that they could not climb to flight level 370.

At 1 h 45, the aeroplane entered a slightly turbulent zone, just before SALPU point.

Note: At about 0 h 30 the crew had received information from the OCC about the presence of a convective zone linked to the inter-tropical convergence zone (ITCZ) between SALPU and TASIL.

The crew dimmed the lighting in the cockpit and switched on the lights *"to see"*. The co-pilot noted that they were *"entering the cloud layer"* and that it would have been good to be able to climb. A few minutes later, the turbulence increased slightly in strength.

Shortly after 1 h 52, the turbulence stopped. The co-pilot again drew the Captain's attention to the REC MAX value, which had then reached flight level (FL) 375. A short time later, the Captain woke the second co-pilot and said *"[…] he's going to take my place"*.

At around 2 h 00, after leaving his seat, the Captain attended the briefing between the two co-pilots, during which the PF (seated on the right) said specifically that *"well the little bit of turbulence that you just saw we should find the same ahead we're in the cloud layer unfortunately we can't climb much for the moment because the temperature is falling more slowly than forecast"* and that *"the logon with DAKAR failed"*. Then the Captain left the cockpit.

The aeroplane approached the ORARO point. It was flying at flight level 350 and at Mach 0.82. The pitch attitude was about 2.5 degrees. The weight and balance of the aeroplane were around 205 tonnes and 29% [Mean Aerodynamic Chord, MAC].

The two copilots again discussed the temperature and the REC MAX. The turbulence increased slightly. At 2 h 06, the PF called the cabin crew, telling them that *"in two minutes we ought to be in an area where it will start moving about a bit more than now you'll have to watch out there"* and he added *"I'll call you when we're out of it"*.

At around 2 h 08, the PNF proposed *"go to the left a bit […]"*. The HDG mode was activated and the selected heading decreased by about 12 degrees in relation to the route. The PNF changed the gain adjustment on his weather radar to maximum, after noticing that it was in calibrated mode. The crew decided to reduce the speed to about Mach 0.8 and engine de-icing was turned on.

At 2 h 10 min 05, the autopilot then the auto-thrust disconnected and the PF said *"I have the controls"*. The aeroplane began to roll to the right and the PF made a nose-up and left input. The stall warning triggered briefly twice in a row. The recorded parameters showed a sharp fall from about 275 kt to 60 kt in the speed displayed on the left primary flight display (PFD), then a few moments later in the speed displayed on the integrated standby instrument system (ISIS). The flight control law reconfigured from normal to alternate. The Flight Directors (FD) were not disconnected by the crew, but the crossbars disappeared.

Note: Only the speeds displayed on the left side and on the ISIS are recorded on the FDR; the speed displayed on the right side is not recorded.

At 2 h 10 min 16, the PNF said *"we've lost the speeds "* then *"alternate law protections"*. The PF made rapid and high amplitude roll control inputs, more or less from stop to stop.

He also made a nose-up input that increased the aeroplane's pitch attitude up to 11° in ten seconds.

Between 2 h 10 min 18 and 2 h 10 min 25, the PNF read out the ECAM messages in a disorganized manner. He mentioned the loss of autothrust and the reconfiguration to alternate law. The thrust lock function was de-activated. The PNF called out and turned on the wing anti-icing.

The PNF said that the aeroplane was climbing and asked the PF several times to descend. The latter then made several nose-down inputs that resulted in a reduction in the pitch attitude and the vertical speed. The aeroplane was then at about 37,000 ft and continued to climb.

At about 2 h 10 min 36, the speed displayed on the left side became valid again and was then 223 kt; the ISIS speed was still erroneous. The aeroplane had lost about 50 kt since the autopilot disconnection and the beginning of the climb. The speed displayed on the left side was incorrect for 29 seconds.

At 2 h 10 min 47, the thrust controls were pulled back slightly to 2/3 of the IDLE/ CLB notch (85% of N1). Two seconds later, the pitch attitude came back to a little above 6°, the roll was controlled and the angle of attack was slightly less than 5°.

The aeroplane's pitch attitude increased progressively beyond 10 degrees and the plane started to climb.

From 2 h 10 min 50, the PNF called the Captain several times.

At 2 h 10 min 51, the stall warning triggered again, in a continuous manner. The thrust levers were positioned in the TO/GA detent and the PF made nose-up inputs. The recorded angle of attack, of around 6 degrees at the triggering of the stall warning, continued to increase. The trimmable horizontal stabilizer (THS) began a nose-up movement and moved from 3 to 13 degrees pitch-up in about 1 minute and remained in the latter position until the end of the flight. Around fifteen seconds later, the ADR3 being selected on the right side PFD, the speed on the PF side became valid again at the same time as that displayed on the ISIS. It was then at 185kt and the three displayed airspeeds were consistent. The PF continued to make nose-up inputs. The aeroplane's altitude reached its maximum of about 38,000 ft; its pitch attitude and angle of attack were 16 degrees.

At 2 h 11 min 37, the PNF said *"controls to the left"*, took over priority without any callout and continued to handle the aeroplane. The PF almost immediately took back priority without any callout and continued piloting.

At around 2 h 11 min 42, the Captain re-entered the cockpit. During the following seconds, all of the recorded speeds became invalid and the stall warning stopped, after having sounded continuously for 54 seconds. The altitude was then about 35,000 ft, the angle of attack exceeded 40 degrees and the vertical speed was about -10,000 ft/min. The aeroplane's pitch attitude did not exceed 15 degrees and the engines' N1's were close to 100%. The aeroplane was subject to roll oscillations to the right that sometimes reached

40 degrees. The PF made an input on the side-stick to the left stop and nose-up, which lasted about 30 seconds.

At 2 h 12 min 02, the PF said, *"I have no more displays"*, and the PNF *"we have no valid indications"*. At that moment, the thrust levers were in the IDLE detent and the engines' N1's were at 55%. Around fifteen seconds later, the PF made pitch-down inputs. In the following moments, the angle of attack decreased, the speeds became valid again and the stall warning triggered again.

At 2 h 13 min 32, the PF said, *"[we're going to arrive] at level one hundred"*. About fifteen seconds later, simultaneous inputs by both pilots on the side-sticks were recorded and the PF said, *"go ahead you have the controls"*.

The angle of attack, when it was valid, always remained above 35 degrees.

From 2 h 14 min 17, the Ground Proximity Warning System (GPWS) *"sink rate"* and then *"pull up"* warnings sounded.

The recordings stopped at 2 h 14 min 28. The last recorded values were a vertical speed of -10,912 ft/min, a ground speed of 107 kt, pitch attitude of 16.2 degrees nose-up, roll angle of 5.3 degrees left and a magnetic heading of 270 degrees.

No emergency message was transmitted by the crew. The wreckage was found at a depth of 3,900 metres on 2 April 2011 at about 6.5 NM on the radial 019 from the last position transmitted by the aeroplane (BEA, 2012, p. 21-23).

The report also concludes that causes of the accident were:

The obstruction of the Pitot probes by ice crystals during cruise was a phenomenon that was known but misunderstood by the aviation community at the time of the accident. From an operational perspective, the total loss of airspeed information that resulted from this was a failure that was classified in the safety model. After initial reactions that depend upon basic airmanship, it was expected that it would be rapidly diagnosed by pilots and managed where necessary by precautionary measures on the pitch attitude and the thrust, as indicated in the associated procedure.

The occurrence of the failure in the context of flight in cruise completely surprised the pilots of flight AF 447. The apparent difficulties with aeroplane handling at high altitude in turbulence led to excessive handling inputs in roll and a sharp nose-up input by the PF. The destabilisation that resulted from the climbing flight path and the evolution in the pitch attitude and vertical speed was added to the erroneous airspeed indications and ECAM messages, which did not help with the diagnosis. The crew, progressively becoming de-structured, likely never understood that it was faced with a "simple" loss of three sources of airspeed information.

In the minute that followed the autopilot disconnection, the failure of the attempts to understand the situation and the de-structuring of crew cooperation fed on each other until the total loss of cognitive control of the situation. The underlying behavioural hypotheses in classifying the loss of airspeed information as "major" were not validated in the context of this accident. Confirmation of this classification thus supposes additional work on operational

feedback that would enable improvements, where required, in crew training, the ergonomics of information supplied to them and the design of procedures.
The aeroplane went into a sustained stall, signalled by the stall warning and strong buffet. Despite these persistent symptoms, the crew never understood that they were stalling and consequently never applied a recovery manoeuvre. The combination of the ergonomics of the warning design, the conditions in which airline pilots are trained and exposed to stalls during their professional training and the process of recurrent training does not generate the expected behaviour in any acceptable reliable way.

In its current form, recognizing the stall warning, even associated with buffet, supposes that the crew accords a minimum level of "legitimacy" to it. This then supposes sufficient previous experience of stalls, a minimum of cognitive availability and understanding of the situation, knowledge of the aeroplane (and its protection modes) and its flight physics. An examination of the current training for airline pilots does not, in general, provide convincing indications of the building and maintenance of the associated skills.

More generally, the double failure of the planned procedural responses shows the limits of the current safety model. When crew action is expected, it is always supposed that they will be capable of initial control of the flight path and of a rapid diagnosis that will allow them to identify the correct entry in the dictionary of procedures. A crew can be faced with an unexpected situation leading to a momentary but profound loss of comprehension. If, in this case, the supposed capacity for initial mastery and then diagnosis is lost, the safety model is then in "common failure mode". During this event, the initial inability to master the flight path also made it impossible to understand the situation and to access the planned solution.

Thus, the accident resulted from the following succession of events:

- Temporary inconsistency between the airspeed measurements, likely following the obstruction of the Pitot probes by ice crystals that, in particular, caused the autopilot disconnection and the reconfiguration to alternate law;
- Inappropriate control inputs that destabilized the flight path;
- The lack of any link by the crew between the loss of indicated speeds called out and the appropriate procedure;
- The late identification by the PNF of the deviation from the flight path and the insufficient correction applied by the PF;
- The crew not identifying the approach to stall, their lack of immediate response and the exit from the flight envelope;
- The crew's failure to diagnose the stall situation and consequently a lack of inputs that would have made it possible to recover from it.

These events can be explained by a combination of the following factors:

- The feedback mechanisms on the part of all those involved that made it impossible:
    - To identify the repeated non-application of the loss of airspeed information procedure and to remedy this,
    - To ensure that the risk model for crews in cruise included icing of the Pitot probes and its consequences;

  - The absence of any training, at high altitude, in manual aeroplane handling and in the procedure for *"Vol avec IAS douteuse"*;
- Task-sharing that was weakened by:
  - Incomprehension of the situation when the autopilot disconnection occurred,
  - Poor management of the startle effect that generated a highly charged emotional factor for the two copilots;
  - The lack of a clear display in the cockpit of the airspeed inconsistencies identified by the computers;
- The crew not taking into account the stall warning, which could have been due to:
  - A failure to identify the aural warning, due to low exposure time in training to stall phenomena, stall warnings and buffet,
  - The appearance at the beginning of the event of transient warnings that could be considered as spurious,
  - The absence of any visual information to confirm the approach-to-stall after the loss of the limit speeds,
  - The possible confusion with an overspeed situation in which buffet is also considered as a symptom,
  - Flight Director indications that may led the crew to believe that their actions were appropriate, even though they were not,
  - The difficulty in recognizing and understanding the implications of a reconfiguration in alternate law with no angle of attack protection.

Note that the listed "Causes of the Accident" focus primarily on the flight crew behavior and the events in the event chain reflecting flight crew actions. A system's approach looks not only at what human operators (such as pilots) did that contributed to the accident but, more important, *why* they believed it was the right thing to do at that time [Dekker, 2017]. Although the latter was addressed, a systems approach will look at these aspects more deeply in that the entire system for preventing a stall is examined and not just the pilot behavior. How did the system design influence the events and the flight crew's behavior? Why were the design controls to prevent a stall not effective in this case?

In this approach, safety is treated as a *control* problem, not a *failure* problem. Commercial aviation has many controls to prevent a stall. To maximize learning from the events, focus in CAST is on why the controls were not effective in this case and how they can be improved for the future.

The rest of this section shows the CAST analysis of the accident causes. As will be seen, most of the emphasis is on explaining why the flight crew and others behaved as they did, i.e., why it made sense to them to do what they did [Dekker, 2017], and why the controls to prevent such behavior were not effective.

CAST tries to avoid *hindsight bias* by assuming that the humans involved (absent any contradictory information) were trying to do the right thing and did not purposely engage in behavior that they thought would lead to an accident. After an accident, it is easy to see where people went wrong, to determine what they should have done or not done, to judge people for missing a piece of information that turned out to be critical, and to blame them for not foreseeing or preventing the consequences [Dekker, 2017]. Before the event, such insight is difficult and, usually, impossible. The Clapham Junction railway accident in Britain concluded: "There is almost no human action or decision that cannot be made to look flawed and less than sensible in the misleading light of hindsight" [Hidden 1990]. CAST attempts to eliminate hindsight bias as much as possible from accident analysis. Simply listing what people did wrong provides very little useful information about how to eliminate or mitigate that behavior.

The next section describes CAST using Air France 447 as an example. In the last section, the BEA findings and recommendations are compared to the CAST findings and recommendations.

There was no opportunity to do additional investigation for the CAST analysis, so the only things used were the BEA findings (which are usually very comprehensive) and the basic knowledge of the authors of this report about aircraft safety and airline operations. The difference is not in the facts but in their interpretation.

CAST is most effective when used during an investigation to generate the questions that should be answered. Many of the questions generated during the CAST analysis are not answered in the BEA report and are therefore left as questions in the CAST analysis. Even without answers to these questions, additional conclusions and recommendations are derived from the CAST analysis than are provided in the BEA report on this accident.

CAST Analysis of Air France 447

In a systems approach to safety, the role of the system as a whole to ensure constraints on behavior (i.e., prevention of hazards) is emphasized, not individual failures. To maximize learning from the events, focus in CAST is on *why* the controls were not effective in this case and how they can be improved for the future.

CAST has three main components: identifying the system-level hazard involved in the loss (usually easy), modeling the control structure involved in the accident, and analyzing the control structure to identify why the existing controls were unable to prevent the accident. The results are then used to generate recommendations to improve the controls and control structure in order to prevent future accidents.

Identifying System-Level Hazard Leading to the Loss

The first step in the CAST analysis is identification of the hazard involved. In this case it was *aerodynamic stall*. The constraint that must be enforced by the controllers and controls is that aircraft must not experience a loss of control.

The next step is to build a model of the safety control structure. The safety control structure is the controls that existed at the time of the accident to prevent the hazard. That control structure will in subsequent steps be used to analyze why it was not effective in this case.

Modeling the Safety Control Structure Created to Prevent a stall (the Hazard)

Aviation has an excellent safety record and learning from past events has led to many controls being introduced into the system. The goal of the CAST analysis is to determine why the controls (as a whole) were ineffective in preventing the current loss. To accomplish this goal, a model is first created of the current controls and overall control structure. This model then becomes the focus of the analysis.

The control structure uses the basic engineering concept of feedback control. Figure 1 shows a simple feedback control loop. The usual requirements for effective management—assignment of responsibility, authority, and accountability—are mapped onto this control loop. The controller has responsibilities assigned to it with respect to enforcing the system safety constraints. It satisfies these responsibilities by issuing control actions on the process it is controlling (representing its authority). The controller can determine what type of control actions are required to satisfy its responsibilities for preventing hazards given the current state of the controlled process, as identified through feedback from the controlled process.

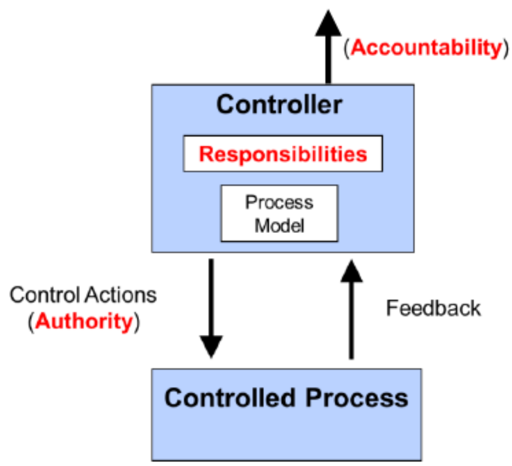


Figure 1: A Simple feedback control loop showing the relationship to standard Management concepts of responsibility, authority, and accountability

As an example, The FAA has responsibilities related to overseeing the safety of flight in the U.S. They have various types of control actions to carry out their responsibilities, such as airworthiness circulars and directives, FAA regulations, handbooks and manuals, Notices to Airmen (NOTAMs), policy and guidance, etc. Feedback comes in the form of reporting systems, accident and incident analyses, audits and inspections, etc. to determine the current state of safety of the air transportation system. Ultimately, they are accountable to the U.S. Dept. of Transportation, Congress, and the executive branch.

Feedback information is incorporated into the controller's model of the controlled process, called the *process model* or, if the controller is a human, it may be called the *mental model*. Accidents often result when the controller's process model becomes inconsistent with the actual state of the process and the controller provides unsafe control as a result. For example, the air traffic controller thinks that two aircraft are not on a collision course and does not change the course of one or both. Other examples are that the manager of an airline believes the pilots have adequate training and expertise to perform a particular maneuver safely when they do not or a pilot thinks that de-icing has been accomplished when it has not.

There are four general types of unsafe control actions:

- A provided control action leads to a hazard: e.g., two aircraft are not on a collision course but ATC issues control actions that put them on one.

- Not providing a necessary control action leads to a hazard: e.g., two aircraft are on a collision course but one or both are not diverted.
- A control action provided with wrong timing (early, late) or control actions in the wrong order leads to a hazard: a change of course is issued, but too late to avoid the collision.
- A continuous control action provided for too long or too short a time leads to a hazard: e.g., the pilot is told to go up to 30,000 feet but instead levels off at 25,000 feet.

These four types of unsafe control actions, along with the hierarchical safety control structure, can be used after an accident to generate the causal scenarios that led to the loss or to identify future potential accident scenarios so they can be eliminated or mitigated in the system design.

Problems can occur not just because of inconsistency between the controller's process model and the state of the controlled process but also when different controllers, all involved in the same general task—particularly under safety-critical or emergency conditions—are operating with different mental models of either (a) what the system is currently doing, or (b) what should be done to control it. Process models are kept up to date, as stated, through feedback or from information received externally. A common factor in accidents is that appropriate feedback or other information about the state of the controlled process is incorrect, missing, or delayed, for example in the Qantas 72 accident the envelope protection system was provided information that the aircraft had exceeded the stall angle of attack, so acted accordingly. Similarly, the pilots of Northwest 6231 reacted to an incorrect airspeed reading and so pulled the airplane up into an aerodynamic stall.

The use of the process model concept is a much better way to understand why humans or software may have done the wrong thing and how to prevent such events in the future than simply saying the human or software or organization "failed," which only attaches a pejorative word without providing any insight about *why* the person or software did something dangerous.

The basic control loop shown in Figure 1 is combined with others to create the more complex control structure in real safety control systems. Figure 2 shows a generic example of a safety control structure. The controls related to development are shown on the left and those relating to operations on the right. The downward arrows represent control actions while the upward arrows show feedback. Each level of the control structure controls the components at the level below.

There is usually interaction between parallel control structures. Manufacturers must communicate to their customers the assumptions about the operational environment in which the original safety analysis was based, e.g., maintenance quality and procedures, as well as information about safe operating procedures. The operational environment, in turn, provides feedback to the manufacturer about the performance of the system during operations. Each component in the hierarchical safety control structure has responsibilities for enforcing the safety constraints appropriate for that component. Taken together, the entire control structure should prevent or mitigate hazardous system behavior.

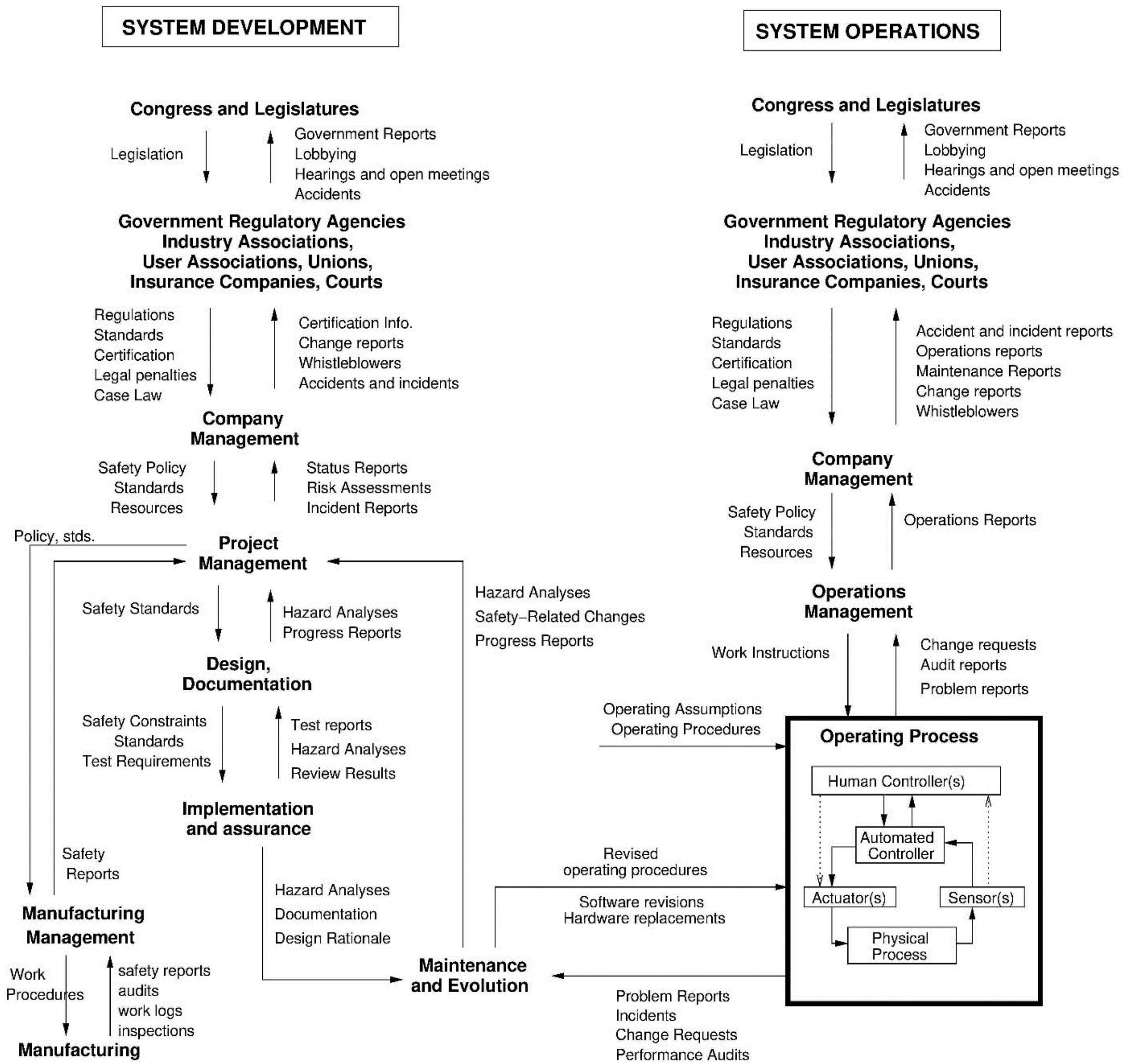


Figure 2: A generic example safety control structure

Note that the use of the term “control” does not imply a rigid command and control structure. Behavior is controlled not only by engineered systems and direct management intervention, but also indirectly by policies, procedures, shared value systems, and other aspects of the organizational culture. All behavior is influenced and at least partially “controlled” by the social and organizational context in which the behavior occurs. Engineering (i.e., designing) this context can be an effective way to create and change a safety culture, i.e., the subset of organizational culture that reflects the general attitude about and approaches to safety by the participants in the organization or industry [Shein 1986].

CAST Analysis of Air France 447

Following the steps for CAST as outlined previously, we will now look at the Air France 447 accident.

Identify System-Level Hazard Leading to the Loss

Aerodynamic stall.

Model the Safety Control Structure to stall (the Hazard)

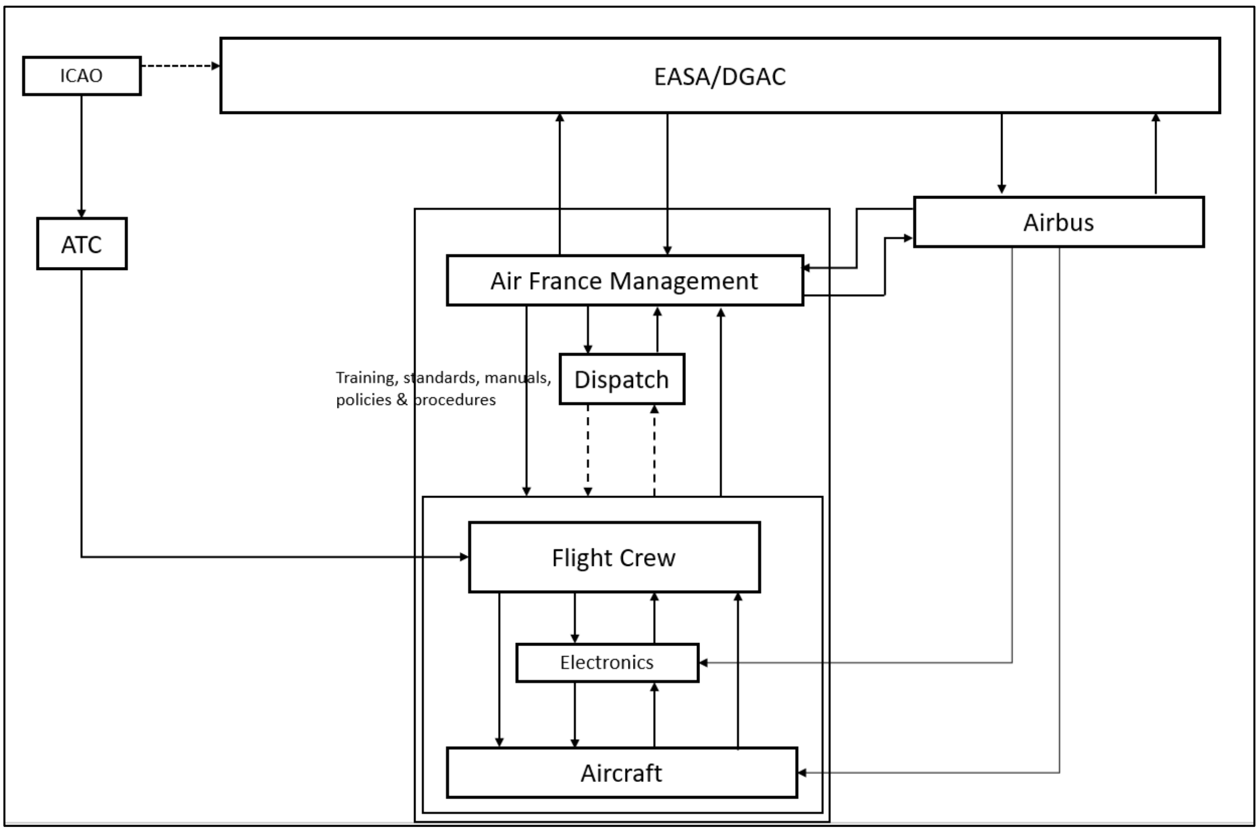
In the case of Air France 447, EASA and DGAC had the responsibility to oversee the safety of Air France flights as well as oversee Airbus. They use their regulatory authority to ensure the handbooks, manuals, policy and guidance are carried out. They receive feedback via various reporting systems, as well as monitoring of the various entities involved. They, in turn, are held accountable by the government of France. EASA, DGAC and the relevant air traffic controllers work in conjunction with a larger framework dictated by the International Civil Aviation Organization (ICAO).

Starting at the bottom, the aircraft is controlled in two primary paths. Components, such as inflight spoilers, landing gear and flaps are controlled directly by the pilots (spoilers can also be moved to aid in roll control by the flight control system, however, not for the purpose of just increasing drag). Rudder also is controlled directly (although there are some electronic functions also working, such as yaw dampers, they are not pertinent for this analysis). For this reason, we show there is a path for the flight crew to control the aircraft directly. Similarly, while most of the pilot feedback is electronic (via flight instruments that get their information from sensors), the pilots do have some direct feedback from the airplane. These would include accelerations and vibrations (which may actually confuse things!), outside visual reference (if available), sounds, odors and the like.

For the A330, most of the control is via the electronic flight control computers. The autopilot can also fly the airplane, and it also controls via the flight control computers. Like cooking a meal with another person, it is important to know what the other "controller" is doing. With a meal we need to know whether the other person already added the salt! With an airplane the pilot needs to know if the other controller is also working, and vice versa. For example, there have been several accidents when both the pilot and the autopilot were simultaneously trying to control the airplane. In each case neither knew the other was trying to fly the plane. As stated earlier, for a human we call this knowledge a "mental model." For the computer it is called a "process model." Either way it adds up to the same thing. An accurate process model is needed to make correct decisions, and that requires accurate feedback.

The "electronics" box represents the autopilot, the flight control computers, and the flight instruments. The "aircraft" box represents both the physical aircraft, but also the physical devices on it, such as elevators, trimmable horizontal stabilizer, ailerons, spoilers, as well as items such as pitot tubes (for feedback).

The pilots are, in turn, controlled (loosely) by their dispatcher (although that is not an instant control), and the dispatcher is "controlled" by the airline management. The airline management is "controlled" by the policies and recommended practices designed by Airbus, who also has direct control over the design of the aircraft and its electronics. The airline management receives direct feedback via its systems on the state of the aircraft (when maintenance is performed), the electronics (both from maintenance as well as electronic datalink) and from the pilots and flight attendants. The airline management then provides information back to Airbus as well as the regulator[4]. Air France is controlled (for the purposes of this accident) by the regulators, EASA and DGAC. Not included on this chart is the fact that the airline is controlled by its shareholders. Of course, the regulators are, in turn, controlled by the government (multiple governments in the case of EASA). The relevant air traffic control was operating under the ICAO rules. EASA and DGAC also operate within the framework of ICAO but that aspect is not pertinent to this accident.



A large part of the CAST analysis is to generate questions to be answered by the investigators. In this case we are generating questions as if this analysis were occurring in real time, however, as it is not, many of these questions remain open. This serves as an example to show that utilizing CAST can provide guidance to the investigators to help broaden the investigation and to organize it in terms of the questions that must be answered.

AIRCRAFT PHYSICAL COMPONENTS

[4] It is unknown if, at the time, Airbus also received direct information from the aircraft. Some manufacturers do receive constant monitoring of airplanes, engines, etc. as part of their quality assurance program, however this does not change the outcome for this accident.

<u>Physical control systems</u>

- Aircraft control surfaces
- Engines

<u>Failures and Contributing Interactions</u>

- No physical component failures on the aircraft contributed to the stall.
- The aircraft stalled and impacted the ocean.
- The elevators were in a position that would cause the aircraft to stall. Angle of attack was too high to prevent a stall.
- Trimmable Horizontal Stabilizer (THS) trimmed to a full-nose up position

<u>Context:</u>

- Elevators were following guidance from the pilots via the flight control system.
- Engines were following the pilot commanded settings or being set via the autothrottle reacting to the pilot selected setting coupled with data from the aircraft systems (airspeed/mach number).
- THS functioned as designed, trimming in response to commands from the flight control computers.

<u>Recommendations</u>: None. This may seem odd but nothing here failed to work as designed and these systems *should* respond as commanded – which they did.

Control actions. Note that there are several sources for these, including the pilot commands and the flight control system. The autopilot would also be possible, but had disconnected.

Pitot tubes (technically part of the physical system but separated out here for analysis)

<u>Responsibility related to stall</u>:

- Provide accurate measure of dynamic pressure to other systems.

<u>Contributing Control Action</u>: Susceptible to blockage by ice crystals [control action not provided].

Why? (Factors Affecting the Contributing Control Action)[5]	Questions Raised
1. Pitot tube design did not consider that ice crystals could be of a size that would create loss of airspeed data. 2. Ice crystals were poorly understood at the time and atmospheric models indicated	*1. Why were larger ice crystals not considered likely?* *2. Why is it standard industry practice to assume that pilots will be able to handle unexpected problems?*

[5] The reasons we list here for the various entities, Airbus, Thales, Air France, etc., are assumptions we have made. In an actual investigation these would be researched by the investigative authority (BEA in this case) to obtain actual answers from the responsible party.

that the probabilities of a larger size ice crystal was very low. 3. The design was very reliable throughout the entire flight regime and changing the design for something that was considered a low probability was deemed less safe. 4. It is standard industry practice to consider that rare or improbable events will be handled by the pilot and part of the certification process (ARP 4761) 5. Design methods followed standard industry practices.	3. *Why wasn't the limitation recognized? And if it was, why were they not replaced before the flight?*

Recommendations:

- Evaluate the certification process to determine whether it is still appropriate in the age of software and increasing complexity of systems. Should the flight crew be included in a more direct way? Is probability the best or only way to assess risk? (consider qualitative means to understand the impact of various events on the system as a whole)

Stall warning system

Responsibility related to preventing stall:

- Provide salient stall warning prior to the aircraft exceeding a stall angle of attack.

Contributing Control Action: Did not provide stall warning continuously when the aircraft was stalled.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Design assumed that a stall warning would be a false indication if the calibrated airspeed was too low. If all three ADR's[6] are lower than 60 knots then the angle of attack values of the three ADR are invalid and stall warning is inoperative. The logic was that airflow must be sufficient for valid measurement by the angle of attack sensors to prevent spurious warnings. 2. Utilizing a different method, such as "weight on wheels" might have created secondary problems for other failure scenarios.	1. *Why was the system designed to eliminate the stall warning if airspeed was below a certain value? What were the design assumptions involved?* 2. *What was the type of engineering analysis utilized to make this decision regarding the stall warning?* 3. *Why was it deemed a better approach to use low*

[6] Air Data Reference

3. Airbus considers that an aural and visual warning is sufficient to alert pilots of a stall as a stick-shaker is problematic on the sidesticks and the envelope protection should prevent the need. In the event of the multiple failures involved to reach the scenario the design assumption is that the pilot will be able to mitigate it. 4. .	*airspeed rather than another mechanism to eliminate false alarms, such as weight-on-wheels.* 4. *Why was there no apparent concern that the pilot might not be able to ascertain where in the envelope they were when they had no feedback from flight controls or other indications of changing speed in the scenario encountered on this flight? Was this scenario ignored or just not thought of?* 5. *Did Airbus utilize standard industry practices in their design?*

Recommendations:

- Change the stall warning such that it activates continuously in flight. Employ a more powerful qualitative analysis methods that include non-failure scenarios, including design flaws and unexpected cases, during the design and certification process.

Flight control system

<u>Responsibility related to prevention from stall</u>:

- Automatically reduce angle of attack if the angle of attack becomes critical.
- Provide pilots with control forces that match their expectations for a stall.
- Provide feedback to the pilots in such a way that they are aware of where in the fight envelope they are.
- Design so that natural stability will allow aircraft to avoid stall.
- Provide handling qualities that meet a minimum value to be determined on the cooper-harper scale.

<u>Contributing Control Action</u>: Did not reduce pitch as angle of attack became critical.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised

1. Due to loss of speed data, the flight control law envelope protection was no longer operating. 2. System reverted to ALT 2B rather than direct law with loss of data. ALT 2B retains the pitch response that is the same as normal law without the envelope protections. This system mode was by design. 3. The design was scrutinized using the best and most current engineering practices, analysis, and risk assessments.	1. *What were the engineering assumptions underlying the design?* 2. *It appears that the intent was to retain as much consistent flying qualities as possible, is that accurate?* 3. *How were the design requirements assessed and validated?*

Recommendations:

- Revert to direct law with data failures so as to ensure the aircraft natural stability will help mitigate stalls.
- Utilize a more sophisticated design analysis and risk assessment that includes human factors (the pilot is part of the overall system design).

Contributing Control Action: Added nose-up trim (THS[7]) as angle of attack increased.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. System is designed to automatically reduce trim drag. The system performed as designed. 2. ALT 2B mode retains normal pitch response, which includes trim. 3. The design goal was to minimize workload for the pilots and therefore a change in the flight control response should be avoided if possible. Maintaining normal response to pitch met this requirement. 4. The automatic trim was part of the design goal of reducing workload. 5. The design was scrutinized using the best and most current engineering practices, analysis, and risk assessments.	1. *Why was the system designed to allow for this combination of factors, i.e. a combination of loss of protections while still maintaining "normal" inputs when the combination could lead to a stall scenario?* 2. *Why does the system allow for automatic trimming when other data is lost?* 3. *What were the engineering assumptions underlying the design?*

[7] Trimmable Horizontal Stabilizer.

Recommendations:

- Disable autotrim with degraded flight control modes to enhance the natural aircraft characteristics to reduce the angle of attack to maintain a safe margin above stall.
- Ensure adequate feedback to pilots of the THS position and movement.

<u>Contributing Control Action</u>: Utilized g-rate (or possibly pitch-rate?) when angle of attack was critically high.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. System reverted to ALT 2B which retains characteristics of normal law in pitch. 2. The mode of the system was by design. It was expected to attempt to maintain consistent handling qualities and other functions that were possible as data was lost.	*1. Why was the system designed to allow for this combination of factors, i.e. a combination of loss of protections while still maintaining "normal" inputs when the combination could lead to a stall scenario?* *2. What were the engineering assumptions underlying the design?*

Recommendations:

- Utilize more sophisticated design tools to analyze potential hazards during development. Potential solutions might include changes such as:
    - Consider revert to direct law with data failures to ensure the aircraft natural stability will help mitigate stalls.
    - Consider modifying the control law such that when in direct law, autotrim is disabled, further enhancing the natural aircraft characteristics to reduce the angle of attack and maintain a safe margin above stall.

<u>Contributing Control Action</u>: Reverted to direct law in roll, increasing pilot workload.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. ALT 2B functionality does not include roll.	*1. Why does it lose roll and not normal response in pitch (aside from protections)?*

Recommendations:

- If analysis shows it necessary to retain pitch mode normal response, accommodations should be made to also retain normal law in roll.

Flight director system

Responsibility related to prevention from stall:

- Present accurate path information to prevent excursion from the flight envelope or bias out of view.

Contributing Control Action: Displayed "pitch up" information when the angle of attack was too high.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Flight director was commanding a path to return to the selected altitude. 2. After the system had lost data it latched onto the previous pitch for the commanded rate of climb. 3. System is designed to maintain the programmed flight path as set on the FCU[8] or FMS.	1. *Why did the flight director command altitude over a safe pitch attitude?* 2. *Why did it default to a pitch up command after the data loss?*

Recommendations:

- Flight director algorithm should command a safe AoA first, then the commanded FCU or FMS path second.
- Review design criteria and assumptions.

Pilot flying (Bonin)

Responsibility related to prevention from stall:

- Avoid area containing high altitude ice crystals
- Maintain pitch attitude below the stall.

Contributing Control Action: Flew into area containing high altitude ice crystals.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised

[8] Flight Control Unit

1. Did not receive training on radar use that included strategies for avoiding convective weather in tropical regions. Pilots receive little or no training on the topic. This is an industry-wide problem and not restricted to Air France. 2. Was not familiar with the risk of high-altitude ice crystals. High altitude ice crystals were poorly understood at the time. 3. He was following the radar guidance as contained in the Air France manuals. 4. He was relying on the pilot monitoring, who was more experienced on the route. 5. He had flown through similar areas in the past and the only problem was turbulence. 6. Radar training is generally poor across all airlines. 7. Pilots receive only minimal training on meteorology.	*1. None.*

Recommendations

- Enhance pilot training for the use of weather radar based on the latest research.
- Improve radar to automatically adjust for regional differences.
- Train pilots as to how thunderstorms may appear in different circumstances and regions of the world.
- Train pilots to understand the actual radar algorithms so they can assess whether the information presented may need additional analysis.
- Provide more weather information to pilots in flight that is updated in real time to aid in decision making.
- Research high altitude ice crystals to improve understanding.

Contributing Control Action: Held nose-up pitch.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Believed that aircraft was not stalled. 2. No feedback to pilot as stall angle of attack was approached and exceeded.	*1. Why did he believe this?* *2. What factors were involved that led to this errant belief?*

3. Control stick is just spring loaded to center so stick forces do not change with variations of speed. 4. May have believed that loss of airspeed indications caused stall warning. 5. May have been attempting to gain more performance with Clmax feature. 6. Was task saturated trying to maintain wings level. 7. Did not trust pitot static instruments 8. May have been following flight director commands 9. Flight director was commanding nose-up. 10. Training did not include the actual physical factors that are involved with a stall at altitude in a transport airplane. 11. Noise levels appeared to correspond to high speed (graupel hitting windshield). 12. G-forces were more analogous to what many pilots felt was a structural failure than a stall, or perhaps heavy turbulence. 13. Weather in thunderstorm had turbulence which made detecting buffet forces difficult. 14. Believed that full nose-up controls would provide Clmax protection (maximum performance as in "normal" law). 15. Believed that roll oscillations were due to turbulence or structural failure. 16. Believed that stall warnings, when they were present, were false (partly due to the fact that they stopped when pitch was increased, and began when pitch was reduced). 17. Believed that what they were seeing and experiencing was weather related, turbulence, etc. (supposition based on other pilots doing this).	3. *Why was there no feedback to pilot?*

Recommendations:

- Train pilots for high altitude handling with degraded flight controls
- Ensure pilots are trained to understand the nuances of high altitude stalls.
- Create training scenarios that allow the aircraft to enter a stall in such a way that the pilot is not aware that it has occurred.
- Train high altitude aerodynamic principles for transport aircraft.
- Improve training for pilots on flight control modes.
- Improve salience of flight control modes.

Pilot monitoring (Robert)

<u>Responsibility related to prevention from stall</u>:
- Avoid area containing high altitude ice crystals
- Monitor or intervene to maintain pitch attitude below the stall.

<u>Contributing Control Action</u>: Flew into area containing high altitude ice crystals.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Did not receive training on radar use that included strategies for avoiding convective weather in tropical regions. 2. Was not familiar with the risk of high altitude ice crystals. 3. He was following the radar guidance as contained in the Air France manuals. 4. He had flown through similar areas in the past and the only problem was turbulence. 5. Radar training is generally poor across all airlines. 6. Pilots receive only minimal training on meteorology 7. *High altitude ice crystals were poorly understood at the time*	*1. None.*

Recommendations
- See PF recommendations.

<u>Contributing Control Action</u>: Did not monitor or intervene to maintain pitch attitude below the stall.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Believed that aircraft was not stalled. 2. Was not aware of PF flight control commands. 3. Had seat fully back and to the stowage position making it difficult to properly reach the controls. Pilots often have their seat moved back for comfort on long-haul flights. 4. Was task saturated with the multiple alerts. 5. Left and right control sticks are not connected, it is difficult to see across the cockpit to be sure what the other pilot is doing; 6. When he did take the controls, they did not appear to be reacting the way he expected. He would push forward and the stall warning would start, leading him to try something else. 7. High rate of descent created urgency and a quick response was required. Pilots were unaware how slowly the aircraft would respond due to full nose-up trim. 8. Pilots are trained to read the alerts and attempt to diagnose the problem. 9. Master caution is one of the visual indications for stall but also used for many other system problems.	*1. Why was he not aware of the PF commands?* *2.* How are design decisions made about the effects of multiple alert overload?

Recommendations (in addition to PF):

- Provide feedback of control stick position to PM (see recommendation under Airbus).
- Recommend that pilots move seats forward during any weather penetration, even if it might seem benign, along with fastening seat belts.
- Redesign alerting system such that pilots receive more clear and less distracting feedback as to the aircraft system state.
- Improve training on CRM between relief pilots as well as define roles.

Captain

Contributing Control Action: Left flight deck prior to weather encounter.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. No weather was apparent on radar at the time he left. 2. There was no indication that there would be a problem aside from possible turbulence. 3. There was no other time that would be good to take his required rest period. 4. The flight was still too far from the weather to indicate any threat. 5. Radar was apparently not set to maximum gain as this is not trained. 6. No rest would increase risk, and taking the last rest period could lead to sleep inertia while flying the approach and landing.	*1. Can better weather information be made available to pilots?*

Recommendations:

- See recommendation for PF regarding weather.
- Research problem of crew rest timing.

Contributing Control Action: Did not return immediately to the cockpit when chimed and stall was encountered.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Likely was still in the lavatory preparing for his rest period. 2. May not have heard the chime. 3. May not have recognized the feelings of an actual aerodynamic stall at altitude.	*1. Why was an emergency protocol not established?*

Recommendations:

- Create a separate "emergency" call system for pilots to return so they know that it requires an immediate response.
- Ensure pilots understand the forces for an actual aerodynamic stall at altitude so they can recognize it.
- Establish protocols for immediate return to the flight deck in emergency situations.

Contributing Control Action: Did not take his seat during the event (after returning to the flight deck), staying in the jump seat.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. May have believed that he would be in a better position to monitor. 2. Rate of descent was so high that he may have perceived he did not have time to change seats. 3. By the time captain got to flight deck the aircraft was falling and experiencing less than 1g. 4. Aircraft was also vibrating due to stall buffet so forces were likely high so may have felt that changing seats would add more risk.	

Recommendations:

- None.

Air France

Contributing Control Action: Did not disseminate the pilot reports of other aircraft that lost airspeed after encountering high altitude ice crystals

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Many airlines do not share individual event reports with their pilots. Broad trends are shared only.	*1. None.*

Recommendations:

- Make the publishing and dissemination to their pilots of event reports mandatory at all carriers.
- Investigate event reports as if they were accidents to ensure that all aspects possible to learn are learned and these lessons applied.
- Ensure carriers incorporate the lessons from these reports into their training.

<u>Contributing Control Action</u>: Did not provide adequate training on stall recovery to pilots.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Industry standard stall training (at the time) included utilizing mostly power to "fly out" of it maintaining altitude. 2. Was not aware of actual stall characteristics and could not properly train it. 3. Simulator modeling was not adequate to train stalls.	*1. Why was the airline training department unfamiliar with actual stall characteristics at altitude?* *2. Why was no data provided to the simulator manufacturers so they could model stalls?*

Recommendations:

- Train pilots to reduce angle of attack and not focus on altitude (being done now).
- Train pilots how to recognize a stall at high altitude in a transport airplane.
- Ensure instructors are trained and monitored to ensure the training is consistent with the most current knowledge and methods.

<u>Contributing Control Action</u>: Did not upgrade pitot tubes in a timely manner.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Was waiting for Airbus to complete analysis. 2. The type of pitot tubes installed were not considered any worse than the newer types for the issue of high-altitude ice crystals. 3. They had already switched from an earlier model of BF Goodrich probes due to problems found with those. 4. All of the models of probes exceeded certification standards. 5. After numerous problems, Air France did push to change them again. This was	*1. What structural limitations are placed on airlines that might inhibit their ability to respond more rapidly?* *2. Is it possible that the SMS methodology could unintentionally slow down the response?*

eventually completed. See the footnote for more detail[9]. 6. Unable to take action absent Airbus approval[10].	

Recommendations:

- None. Air France did all that could reasonably be expected given what was known at the time.

<u>Contributing Control Action</u>: Did not provide adequate training on radar and weather.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. No airlines are providing more than minimal training on weather or radar use.	*1. Why is this the industry norm?*

Recommendations:

- Create robust training modules to make sure pilots understand the radar as they do other systems.
- Train pilots on the dynamics of meteorology based on the most current research, with particular attention to convective weather, vertically integrated water and reflectivity differences in various parts of the world.

[9] From the BEA report: On 24 November 2008, the issue of inconsistent airspeed indications was raised during a meeting between the technical divisions of Air France and Airbus. Air France requested an analysis of the root cause and a technical solution to resolve this problem, and suggested that BF Goodrich probes should be fitted, since their reliability appeared to be greater. Airbus confirmed its analysis and agreed to check the option of replacing the Thales probes with BF Goodrich probes.

[10] From the BEA report: On 15 April 2009, Airbus informed Air France of the results of a study conducted by Thales. Airbus stated that the icing phenomenon involving ice crystals was a new phenomenon that was not considered in the development of the Thales C16195BA probe, but that the latter appeared to offer significantly better performance in relation to unreliable airspeed indications at high altitude. Airbus offered Air France an "in-service evaluation" of the C16195BA standard to check the behaviour of the probe under actual conditions.

Air France decided to extend this measure immediately to its entire A330/A340 longhaul fleet, and to replace all the airspeed probes. An internal technical document was drawn up to introduce these changes on 27 April 2009. The modification work on the aircraft was scheduled to begin as soon as the parts were received. On 19 May 2009, based on this decision, the monitoring of these incidents was considered closed during the RX2 meeting. The first batch of Pitot C16195BA probes arrived at Air France on 26 May 2009, i.e. six days before F-GZCP crashed. The first aircraft was modified on 30 May 2009.

<u>Contributing Control Action</u>: Did not provide adequate training on degraded flight control modes.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Training for degraded flight control modes was approved and based on historical data. Very little of this included handling qualities at altitude.	*1. Why are degraded flight control modes not more broadly trained?*

Recommendations:

- Include training for degraded flight control modes in all advanced aircraft equipped with electronic control systems, to include handling qualities at high cruise altitudes in addition to takeoff and landing.

<u>Contributing Control Action</u>: Did not provide adequate dispatch oversight to aid in weather avoidance.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Weather reporting over oceans is not granular enough to enable dispatch to provide much beyond very general guidance.	*1. Can better weather information be obtained?*

Recommendations:

- Dispatchers should attempt to provide all available support on every flight.
- Dispatch centers should retain professional meteorologists to support dispatchers.

Airbus

<u>Contributing Control Action</u>: Designed a flight control system that would degrade with no protections.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. System design was in accordance with industry best practices.	*1. Why do current industry standards not effectively consider complex interactions in electronic systems?*

	2. *Have certification and standards kept up with changes to aircraft design, particularly the integration of software systems?*

Recommendations:

- Consider modifications that would enhance pilot awareness of the actual aircraft state.
- Consider adopting more powerful analysis and design tools, particularly for software and software requirements.

<u>Contributing Control Action</u>: Designed a stall warning system that would deactivate at low airspeeds.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Followed standard engineering practices in design.	1. *Why was the scenario for low airspeed missed in the analysis?*

Recommendations:

- Redesign stall warning system algorithms to make sure systems do not deactivate at low airspeeds in flight.

<u>Contributing Control Action</u>: Designed a flight control system that would continue to automatically trim in degraded flight control modes.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Automatic trim needs to function as part of normal law response in pitch only.	

Recommendations:

- Redesign software to make sure that automatic trim is disabled out of normal law.
- Use more powerful avionics analysis and design tools that consider more than just failures and include sophisticated human factors analysis.

<u>Contributing Control Action</u>: Designed control sticks that are not connected and did not provide any alternative feedback to the monitoring pilot.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Apparently conducted analysis that did not find the need for feedback between pilots necessary.	*1. What were the assumptions for this?*

Recommendations:

1. The stall was initiated by a "too long" control action on the part of the pilot flying. A control action of this nature would not be salient to the pilot monitoring even if the side-sticks moved together. To provide feedback a visual electronic display would be more prominent. Such a display need only be shown on the pilot monitoring's side as the pilot flying already has direct tactile feedback as to what control actions are being made. Sensors are able to detect which pilot is manipulating the controls. The recommendation generated here is that the pilot monitoring display should automatically display flight control positions during the following conditions:
   a. AoA very near to or exceeding the stall AoA.
   b. Full control deflection is commanded (control stick to the stop).

<u>Contributing Control Action</u>: Did not provide upgrades to the pitot system in a timely manner.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Rapid response can create secondary hazards. OEMs need to fully assess all of the factors and the new design prior to making such changes. See footnotes on this issue for Air France.	*1. Did safety policies and practices possibly inhibit a more rapid response?*

Recommendations:

- See previous recommendations.

<u>Contributing Control Action</u>: Did not share full stall data package with simulator manufacturers.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Believed that sharing that information was not necessary.	*1. Why would this information not have been shared?*

Recommendations:

- Manufacturers should retain and share with simulator manufacturers the actual aircraft stall data for training purposes.

EASA
Responsibilities?

Contributing Control Action: Used certification procedures that are not capable of assessing complex interactions, especially those involving software and humans.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Historical practice and industry standard methods were utilized.	

Recommendations:

1. Review and monitor the assumptions used in the design of standards and revise them if the assumptions do not match the current state of the industry.

Contributing Control Action: Did not require that information be retained and shared between OEMs and Airlines.

Why? (Factors Affecting the Contributing Control Action)	Questions Raised
1. Historical data had not shown a need?	*1. Was there a basis or have the assumptions just changed over time?*

1. Share such data among all carriers, worldwide, through a central clearing house, such as FAA's ASIAS (Aviation Safety Information Analysis System), ran by ICAO.
2. Provide such deidentified data to all pilots, to include internal reports.
3. Provide a means to include all technical and internal engineering problems to the database as well through mandatory reporting (currently much of what occurs within an airline is not shared).
4. Require OEMs share full flight test envelope data with simulator manufacturers.

Factors spanning system components

INDUSTRY AND ORGANIZATIONAL SAFETY CULTURE

The industry has moved away from robust systems training and so-called "rare events" in favor of training that is based on statistical trends and estimated likelihood of problems. The manufacturers rely on pilots to manage events considered unlikely. This combination results in pilots not being trained for the same events manufacturers expect them to manage.

Recommendations:

(1) Manufacturers should ensure, and regulators should require, that any assumptions made on what pilots are expected to manage in rare events is effectively communicated to the operators of the airplanes. Regulators should mandate that pilots are trained in all these areas regardless of their role on the flight deck.

SAFETY INFORMATION SYSTEM

There is concern that the sharing of information with pilots can create secondary problems, so it is fairly common for pilots not to be informed of problems experienced by other crews within their airline and industry-wide absent a major event such as a Boeing 737 Max accident. However, it is not possible for pilots to be proactive without this information. Sharing the information encourages pilots to consider the scenario and imagine how they might handle it. This increases their ability to manage novel situations.

Recommendations:

(2) Regulators should ensure that these reports are shared anonymously not just within an airline but with all operators of a particular fleet type.

DYNAMICS AND CHANGES OVER TIME

1. Weather modeling is inadequate with many gaps still apparent in our knowledge base. Designs of highly integrated electronic systems in automation can lead to unexpected interactions that were not considered in the design.
2. More senior pilots who have more experience with managing unusual events are retiring from the industry, leaving behind newer pilots who have not had the opportunity to experience a variety of aircraft handling characteristics, high altitude handling qualities and failure modes (due to the much higher reliability of newer aircraft.
3. Regulations and certifications standards have not kept up with advances in technology. Changes in regulations require an enormous amount of time, almost guaranteeing that they will be obsolete much of the time.

Recommendation:

1. Industry should study their design assumptions and consider a better approach that would consider complex dynamics and effectively manage those problems that are considered "unknown unknowns". Such techniques do exist (e.g., STPA).

2. The airlines and regulators should study improved ways to train newer pilots to make sure they have the ability to cope with unusual and very rare events that may require deep system knowledge and the ability to manage diverse handling qualities. 3. Industry should devote more funding to research gaps in our knowledge of weather phenomena. 4. Regulators should update regulations and standards to meet current needs and monitor the industry for any advances that make those regulations obsolete and unable to address those changes.
COMMUNICATION AND COORDINATION AMONG CONTROLLERS
(1) The ability for the pilots to understand the dynamics were directly affected by lack of feedback between each other, particularly on the control position. (2) Manufacturers and airlines have not shared their assumptions in training and design. **Recommendations**: (1) Improve feedback to the pilots for each other's actions to allow for better assessment of the problems. (2) Improve training for pilots to be able to better communicate issues in novel scenarios. (3) Mandate that airlines and manufactures communicate their assumptions to airlines and regulators so training can be adjusted as necessary to accommodate those assumptions. (4) Ensure manufacturers provide the information to airlines so that pilots can be trained to have a robust understanding of flight control laws so they can anticipate

======================

Comparison of the BEA Results and the CAST Results

We compare only the recommendations generated here. The reader is urged to reference the BEA report itself. Again, no criticism of the BEA report or method should be implied. Their investigations are always first class. We are simply suggesting that the industry as a whole could learn more by using new approaches to accident analysis that were not available at the time of the AF 447 accident report.

The BEA report and CAST analysis contain similar recommendations in many respects. This is not surprising as the CAST analysis started from the BEA report. A better comparison would be to do the analyses in parallel, but that was not possible here. The CAST analysis resulted in additional recommendations. Some of these are similar to the BEA recommendations but are more detailed because of the more extensive CAST causal analysis about why contributory control actions occurred. CAST provides a format and methodology for exploring the causes more extensively and recording the detailed analysis that was used in deriving the conclusions. Other CAST recommendations raise totally different issues as is evident here. This CAST evaluation did not explore the aspects pertaining to improving future accident investigations.

Safety Recommendations	Included by BEA	Included by CAST?	Comparison
Pitot tube design	Yes	Yes	Both the BEA report and CAST found the pitot tubes to be problematic.
Stall warning system	Yes	Yes	Both CAST and BEA called for a review of the stall warning system.
Flight control system	No	Yes	Several CAST recommendations pertained to flight control aspects, including feedback and states after loss of data that would give the pilots a better sense of where they were in the flight envelope.
Flight director	Yes	Yes	Both CAST and BEA called for a review of Flight Director commands.
Weather radar	No	Yes	CAST recommends improvement of inflight weather tools for pilots, including automated weather radar that would detect convective storms in the region the accident occurred.
Weather training	No	Yes	CAST calls for training of pilots to ensure that they can have a better chance avoiding severe weather in the area that the accident occurred.
Pilot training	Partial	Yes	The BEA report addressed the following aspects: 1. Manual handling for approach to stall and stall recover including high altitudes. 2. All aspects of flight control laws and regimes. 3. Specifics particular to the aircraft type. 4. Theoretical knowledge of flight mechanics. 5. Manage surprise generated from unexpected situations. 6. Improve CRM training to enable adequate acquisition and maintenance of automatic responses to unexpected situations. 7. Standardize instruction. The CAST analysis also included aspects such as radar and weather training.
Instructor training	Yes	Yes	Both CAST and BEA recommend ensuring instructors provide consistent and high quality training.
Seat position enroute	No	Yes	CAST recommends that training and policy and procedure be implemented to ensure that pilots

			can adequately reach the controls during cruise portions.
Crew rest periods	Yes	Yes	Both reports recommend reviewing crew rest timing protocols.
Return to seat emergency signal	No	Yes	CAST recommends developing a method to immediately call a pilot back to the flight deck regardless of where they might be on the aircraft.
Event reporting	Yes	Yes	Improve analysis of event reporting by flight crews.
Flight simulation	Yes	Yes	BEA recommended that simulators be modified to improve fidelity.
Angle of attack display	Yes	Yes	Both reports call for investigating the implementation and training for angle of attack displays to improve pilot situational awareness.
High altitude ice crystals	Yes	Yes	Both reports call for more research into high altitude ice crystals.
Relief pilot defined roles	Yes	Yes	Both reports recommend reviewing the relief pilots roles and the interface between the relief pilot and the other pilots with augmented crews.
Aircraft alert and warning systems	Yes	Yes	Study having a dedicated warning to the crew when specific monitoring is triggered in order to facilitate comprehension of the situation.
System Issues			
Industry and organizational safety culture	No	Yes	CAST recommends reviewing assumptions that are made in the design and ensuring that manufacturers share these assumptions with operators.
Safety Information System	Yes	Yes	Regulators should ensure that safety reports are disseminated to all flight crews at all operators.
Dynamics and Changes over Time	No	Yes	The CAST analysis recommends that: 1. Industry should study their design assumptions and consider a better approach that would consider complex dynamics and effectively manage those problems that are considered “unknown unknowns”. Such techniques do exist (e.g., STPA). 2. The airlines and regulators should study improved ways to train newer

			pilots to make sure they have the ability to cope with unusual and very rare events that may require deep system knowledge and the ability to manage diverse handling qualities. 3. Industry should devote more funding to research gaps in our knowledge of weather phenomena. 4. Regulators should update regulations and standards to meet current needs and monitor the industry for any advances that make those regulations obsolete and unable to address those changes.
Communications and coordination between controllers	No	Yes	(1) Improve feedback to the pilots for each other's actions to allow for better assessment of the problems. (2) Improve training for pilots to be able to better communicate issues in novel scenarios. (3) Ensure manufacturers provide the information to airlines so that pilots can be trained to have a robust understanding of flight control laws so they can anticipate

Summary and Conclusions

This report has described a new method to provide a structured approach to accident causal analysis called CAST. The new approach is based on a more inclusive model of accident causation that focuses on more than failures but instead generalizes from failures to look at inadequate control. An example is provided by applying CAST to the stall accident of a Air France 447 on June 1st, 2009.

The results of the case study are compared to the official BEA report on this accident. In general, CAST goes beyond just stating what failures occurred and focuses more on why the events occurred. The findings of both are compared. There are more recommendations that are generated by the CAST analysis. Some are simply more detailed because using the extra information generated by looking more carefully at "why." Others are related to factors that are left out of the BEA findings. We have no information about why they were omitted; there may be very good reasons for this omission. Our goal was simply to demonstrate a new approach to analyzing accident causes.

References:

(BEA) et d'Analyses, B. D. E. (2012). Final report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro–Paris. *Paris: BEA*.

Dekker, S. (2017). *The field guide to understanding 'human error'*. CRC press..

Nancy G. Leveson, Engineering a Safer World, MIT Press, 2012.

Nancy G. Leveson, A systems approach to risk management through leading safety indicators, *Reliability Engineering and System Safety*, 136: 17-34, April, 2015.

Nancy G. Leveson, CAST Handbook, downloadable from http://psas.scripts.mit.edu/home/