Flight Envelope Protection for Automatic and Augmented Manual Control

Antonius A. Lambregts*

Abstract Loss of Control (LOC) is currently the largest contributing category of catastrophic airplane accidents. A large percentage of the LOC accidents involve general aviation airplanes. The FAA is therefore has sponsored research to develop certification requirements for add-on envelope protection functions. This paper briefly discusses some of the LOC accidents and the deficiencies existing in many of the current GA and Transport airplane guidance and control systems that can lead to LOC. Next the paper discusses Envelope Protection (EP) design requirements, as well as functional, safety and performance objectives and design guidelines. Various approaches to designing envelope protection functions are discussed for airplanes under automatic or augmented manual Fly by Wire (FBW) control, to prevent stall, overspeed, excessive pitch and roll attitudes and excessive Normal Load Factor (NLF). Examples of simulation time history of what can be achieved are included.

1 Introduction

In spite of the large strides made in recent years to improve flight safety, Loss of Control (LOC) continues to be the largest contributing cause of accidents and incidents. Loss of Control can occur during airplane operations under automatic and under manual control, on airplanes with conventional control systems, or FBW control systems. LOC accidents and incidents can be attributed to many causes, including pilot error, airplane upsets, design malfunctions, design deficiency.

LOC accidents and incidents can be further classified by main types:

- airplane stall during manual speed control
  - pilot mishandling (e.g. excessive bank angle at low speed) or neglect
  - loss of spatial orientation leading to stall and spin
- airplane stall during operations with automatic or partially automatic control
  - partial automation – flight crew manually controlling trust/airspeed
  - full automation – flight crew selecting excessive climb rate command
- lateral directional control upsets due to
  - atmospheric conditions (e.g. wake turbulence)
  - partial automation – control asymmetry due to icing, engine out, fuel imbalance
- overstressing the airplane structure
  - mishandling during atmospheric upset (e. g. rudder control wake vortex encounter)
  - mishandling during stall recovery
  - excessive Normal Load Factor (NLF) maneuvers, e.g. firefighting flight operations
- exceedance of the high speed airplane limits
  - partial automation – flight crew manually controlling trust/airspeed
  - full automation – flight crew selecting excessive descent rate command
- failure of critical flight control function(s) due to
  - design deficiencies
  - hardware failure

A more comprehensive overview and analyses of airplane upsets and LOC accidents is presented in **[1, 2]**. Many LOC accidents and incidents do not fit neatly into the above classifications and are the result of many contributing factors and circumstances. Often pilot error is cited as the main cause, because the accident or incident could in principle have been avoided by appropriate and expected pilot intervention. However, this ignores the realities of human failure and neglects the fact that in many cases better systems design might helped the pilot to avoid errors. This applies to airplane operations of all categories and levels

* FAA Chief Scientific and Technical Adviser for Advanced Control

of technology. Better pilot training and operational safety standards can reduce, but never completely eliminate pilot errors that can lead to an accident or incident.

Lack of visual cues can lead to spatial disorientation during manual control operations in low visibility conditions, leading to overbanking, stall and spin. Such LOC situations have a very low successful recovery probability. Simple pilot alerting by oral, tactile and visual alerting cues can go a long way to reduce the probability of LOC in these situations.

Mishandling of the rudder control by the pilot of an A300-600, after a relatively mild lateral direction airplane upset during a wake vortex encounter caused the rudder structural limit to be exceeded, resulting in a crash.

There have been numerous airplane accidents and incidents under full and partially automated flight guidance and Control. Some cases are cited below.

Finally, there have been several crashes of Fly By Wire (FBW) equipped airplanes with stall and NLF protection functions, due to system failures and crew difficulties managing the airplane after the failure(s) occurred (AF A330 Flight 447 precipitated by loss of air data due to pitot system icing, Perpignal A320 crash precipitated by frozen Angle of Attack (AOA) vanes).

Therefore further airplane operational safety improvements must and can be realized, mainly by better systems design that will help pilots avoid serious errors and protect the airplane against entry into unsafe operating conditions by the application of Flight Envelope Protection and Pilot Alerting functions. There is a general worry that this leads to more automation and erosion of manual flying skills and that the additional EP functionality will result in more failure modes and a further increase automation complexity – a valid concern!

In order to mitigate the number of LOC accidents on general aviation airplanes, the FAA has recently sponsored research to find an affordable way to provide envelope protection control force cuing for the pilot to prevent airplane stall and overbanking. The first phase of this research has demonstrated the feasibility of the force cueing and pilot alerting approach. The intend was to minimize the need of new equipment by using the existing autopilot servo, but the results indicated that a more sophisticated servo was required. Follow on research is planned to mature the force cuing concept and extend this concept to legacy transport airplanes **[3]**. The FAA is also sponsoring additional research to improve pilot low speed awareness.

2 Automation Issues

Airplane stall. Today, airplane stalls still occur with a surprising regularity, even in transport airplane operations, both during manual and automatic control. When stall warning occurs at ~1.05Vstall, the airplane is already well below the normal operating speed and in some cases too slow to allow a safe recovery (e.g. Turkish Airline B737 crash in Amsterdam). *There is no defensible justification for letting the airspeed drop significantly (as much as 20 knots) below the intended safe operating speed: corrective action should be taken no later than when the airspeed drops below 1.25Vstall, or there about. As a minimum this action should include the unequivocal alerting of the flight crew.*

Traditional SISO-basedAutomatic Control. The current generation of automatic Flight Guidance and Control (FG&C) systems are the result of 100 years of system evolution that started with very basic airplane stabilization functions. With each new generation more functionality has been added, often to overcome the limitations of the previous design generation. As a result today's systems have become exceedingly complex with too many overlapping modes, each designed to control a single airplane variable for a specific flight condition or operating scenario, using Single-Input/Single-Output (SISO) control technology. Many of these traditional flight control modes stem from different era and have used a variety and sometimes conflicting design approaches. Historically, flight control automation has been

approached axis by axis, one function at a time, without an overarching pilot-like airplane control strategy. Currently, the airplane control automation approach is analogous to assigning control of pitch, roll, yaw and airspeed each to a different pilot, with little or no communication between them. Obviously, this is very different from the way pilots control airplanes and not always conducive to instilling confidence that the automation is doing the right thing. As a result the pilots, who are the receiving end of this complex technology, must act as the system user and operations integrator of last resort. Most of the FG&C automation functions are considered "non-flight critical". This means that the flight crew is assumed to recognize and safely manage any failure of function of such modes. However, too often this assumption has proven to be unwarranted. As a result there have been too many automation related incidents and accidents, due to stall, roll divergence after an engine failure, icing etc. The current generation of FG&C systems do not take full advantage of modern MIMO control strategies to functional integrate all modes, eliminate well known safety deficiencies (e.g. by incorporating full flight envelope protection).

Partial Automation. Partial automation, whereby the speed control is left to the flight crew, has contributed to an unacceptably high incidence rate of airspeed mismanagement resulting in airplane stall or overspeed. All of today's Fight Guidance and Control systems include open ended vertical flight path control modes that are based on the Single Input/Single Output (SISO) control concept that can be used for convenience and crew workload relief. Simple SISO vertical path control modes can only control the vertical path as long as the required thrust is provided, either manually, or by the Autothrottle. Even when the Autothrottle is controlling the airspeed, the airspeed can diverge if the flight crew selects a vertical speed command outside airplanes performance capability with thrust at the upper or lower limit. This can happen even with a moderate vertical speed command, because the maximum thrust will fall off as the airplane climbs out (Air Mexico DC10 accident after departure from Frankfurt, Germany). Therefore the safety of operation of these modes is critically dependent on the flight crew providing the complementary thrust control, monitoring and intervention functions. Pilots may assume the airplane is under "full automatic control" letting their attention slip, or when the autothrottle is off forget to re-trim the throttle after an automatic level off and Altitude Hold mode engagement, causing the speed to diverge toward stall. This type of LOC risk has been mitigated on more recent transport and high end GA airplanes by the introduction of a Flight Level Change (FLCH) mode. However, the Glide Slope mode is still vulnerable to LOC, e.g. Colgen Air DHC-8-400 crash at buffalo NY; Turkish airline B737 crash in Amsterdam.

In the latter case, the airplanes autopilot captured and began tracking the Glide Slope, the autothrottle was on and set to the correct speed command, but the radar altimeter signal that controls the throttle retard during automatic landing failed, providing a false low altitude reading. This triggered the throttles to retard. None of the three pilots on board noticed this, nor did they properly monitor their flight instruments. In such cases the autopilot will do all it can to maintain the commanded flight path. With inadequate thrust the speed will run down and the autopilot will cause the airplane to stall. For the Turkish B737 the stall warning occurred at ~400 ft altitude, too late to recover in the flaps down, high drag final approach configuration. The airplane crashed. The pilots were justifiably blamed, but that should not have been the end of the story. Pilot errors will occur. Better system design could have helped the flight crew to avoid the accident. It is likely that the following simple improvements in the FG&C system would have prevented the accident:
1) *the flight crew should be alerted as soon as the speed drops significantly below the intended safe operating speed, e.g. for V< ~1.25Vstall;* ***2)*** *the throttle retard was a single point failure of a radar altimeter, a second one was on board and should have been used for cross monitoring to detect failures;* ***3)*** *the design should not have allowed the automatic throttle retard function to be activated, because no automatic landing was planned;* ***4)*** *safe automatic Glide Slope control cannot be assured without an appropriately functioning automatic thrust control. For such conditions the flight crew must be made aware of the critically important complementary manual thrust control task they need to perform to maintain safe operation.*

Curiously, whereas the CFRs require that the basic unaugmented airplane dynamics be unconditionally stable in all degrees of freedom and in all plight phases, the Certification Authorities have never mandated that during operations with partial or full control automation the airplane should also be unconditionally stable and free from tendencies to diverge into stall or overspeed,

assuming fault-free operation. FAR 25.1309 § a) : *"The …systems must be designed to assure that they perform their intended function under any foreseeable operating condition…"* could have been applied to disallow use automation functions that can cause stall during normal fault free operation.

Partial automation of the lateral-directional directional control axes using a roll autopilot with limited control authority and a simple yaw damper with limited rudder control authority and no automatic re-trim capability has contributed to a number of airplane upsets. The yaw damper cannot prevent the build up of a large sideslip angle which induces a large rolling moment on swept wing airplanes. The rolling moment due to sideslip then overwhelms the autopilot roll control authority. Pilot intervention is required for this condition to prevent the airplane from going out of control. A China Airlines B747SP on route to San Francisco experienced such a LOC incident. It went into a spiral dive, but after loosing more than 20,000 ft of altitude the pilots managed to recover the airplane to a normal flying condition and landed safely in San Francisco. In the recovery the pilots pulled 4.3 g. Luckily, the airplane was at the end of a transoceanic flight, therefore relatively light, so it did not break up, but it was "reshaped" permanently.

Abrupt autopilot disengagement due to saturation of is roll control authority has led to several accidents in asymmetric icing conditions. When the autopilot holds a large aileron command and the autopilot disengages, it leaves the airplane out of trim, precipitating an unrecoverable roll (Roselawn ATR72-212 crash; Comair EMB120 crash near Detroit).

Several pitch upsets have occurred during fully automated flight due to combinations of failures and design deficiencies in the functionality for detecting and managing failures (Malaysian B777 and Quantas A330 pitch upsets).

There have been several crashes during fire fighting operations due to the flight crew executing maneuvers with excessive Normal Load Factor, causing structural failure of the wing.

FBW Augmented Manual Control design. With the introduction of FBW augmented manual control designs, envelope protection features have become imperative for designs that utilize non-classical control augmentation, such as Nz-command, C* and Flight Path Angle (FPA) command algorithms. Airplanes equipped with these control concepts lack static longitudinal stability and thus have no definable "trim speed". Therefore, after the application of even a momentary one sided pitch control input while keeping thrust constant, the airspeed will divergence unboundedly from the initial equilibrium speed condition. Such designs do not meet CFR 25.173 and therefore can only be certified by a Special Condition (SC) that requires automatic stall and overspeed protection to achieve an "Equivalent Level of Safety", compared with conventional speed stable airplanes.

Pilot Authority. There is great apprehension in the transport airplane pilot community about "encroaching automation" and especially envelope protection interfering with the ability of the pilot to control the airplane and being able to utilize the full performance capability of the airplane in case of an emergency, e.g. a CFIT or mid-air collision avoidance maneuver [**4, 5]**. The US Airline Pilots Association (ALPA) expressed their conviction as follows [**4]** :

"*The pilot in command must have the authority to obtain maximum available system and aircraft performance, in conjunction with safe operation of the aircraft, under all flight conditions. Aircraft protection systems should be designed to allow pilots easy access to the normal operating envelope of the aircraft and its systems. A straightforward and intuitive disengagement scheme must always be available to allow the pilot increased control authority up to structural or aerodynamic limits in an emergency situation*."

Clearly, many pilots are under the impression that "Hard Envelope Protection" curtails the pilot control authority and reduces the inherent airplane performance capability. Some pilots fear that "Hard Envelope Protection" can get in the way of normal control of the airplane, due to possible design flaws and malfunctions. However these concerns apply to both "Hard" and "Soft" envelope protection methods, driven by design complexity, the number of failure modes, failure mode effects and the probability of design flaws and hardware failures. Each design has its own specific limitations, but it is a misconception

to think that a "Hard Envelope Protection" design curtails access to the inherent airplane structural or aerodynamic performance capability. This issue is discussed in more detail below.

Soft Flight Envelope Protection. On the Boeing FBW airplanes "Soft Envelope Protection" is provided by increasing the control inceptor force gradient as a force cue to the pilot not to pull or push any further when the limit NLF or AOA or high speed limit is approached. For this design the pilot can override the "soft protections" and stall the airplane, overspeed it, or exceed the design NLF (at high speeds), if persistent enough. The approach requires a rather complex and heavy active inceptor force control system with many new failure modes. A real advantage of the system is the ability to provide force cuing when the second pilot applies a control force. During the B777 development British Airways registered there dismay that this approach condemned the airplane to carry around several hundred pounds of extra "dead weight", when they preferred to carry a couple more paying passengers instead. Older pilots often express a preference for "Soft Flight Envelope Protection" over "Hard Flight Envelope Protection", in the belief that they can go closer to the absolute performance limits of the airplane and thus have a better chance to escape harm, in an emergency pull up maneuver. In practice it has not worked out that way. The appeal of "Soft Flight Envelope Protection" may also have been promoted by a clever marketing claim that "Soft Envelope Protection" leaves the "final authority" to the pilot.

Hard Flight Envelope Protection. On the Airbus airplanes "Hard Envelope Protection" functions are provided as part of the FBW augmented manual control system. "Hard Envelope Protection" means that the pilot cannot command maneuver rates in excess of the safe airplane capability and these maneuvering limits are built into the envelope protection functions. This approach is compatible with the use of passive control effectors, which have the advantage of light weight and relative simplicity. A disadvantage of passive control inceptors is that they feature a fixed force versus deflection relationship, which cannot be tailored to the flight condition to achieve the optimum "stickforce/g" relationship, at least not without severe limitations, e.g. large control effector "flat spots" (no change in output command for a change in effector deflection). Furthermore, the control effector input of both pilots must be summed or averaged to develop the airplane maneuver command and no force cueing can be provided when the second pilot applies a control force, except by the use of a vibrator cuing device on the control effector. This has led to "who is controlling the airplane" issues. The Airbus FBW airplanes use Angle of Attack (AOA) to provide stall protection and NLF command authority limiting to prevent excessive NLF, but this NLF command authority limit is not adapted to the actual airplane weight. There have been several AOA protection engagement/disengagement design issues. In order to prevent AOA-limit overshoot, AOA- rate is used to provide early engagement before the actual AOA limit is reached. Airbus also allows the AOA function to operate during the landing flare maneuver. This issue was at the heart of the A320 crash at Bilbao [6], Spain, where the AOA protection engagement due to atmospheric disturbances prevented the pilot from executing a successful landing flare maneuver. For the early design AOA protection engagement was latched in and disengagement was triggered by a nose down command. This became an issue in a near miss incident between an A340 and an A330 over the North Atlantic [7], when the AOA protection engagement was triggered and latched during an atmospheric disturbance, causing an uncommanded climb. The design has since been modified to eliminate engagement latching and to allow the AOA protection to take control only when it develops a command that is more nose down than the basic FBW control algorithm maneuver command. There have been several other LOC accidents and incidents of FBW equipped airplanes:

- the crash of AF A330 Flight 447 precipitated by loss of air data due to icing of the pitot system, reversion to an alternate control law without envelope protection and subsequent crew difficulties managing the airplane
- the crash of an A320 crash into the Mediterranean Sea near Perpignal precipitated by frozen AOA vanes)
- an uncommanded pitch down and LOC incident on an EVA A320, MSN693 due to iced up/frozen AOA-vanes, recovered by pilot after shutting down all three Air Data Reference systems. In this incident the pilots turned off all three ADRs and regained control with only seconds to spare.

Related issues include: *1) the Horizontal Stabilizer Trim (HST) system should be inhibited at low speed, otherwise the HST may trim to its Nose Up stop during approach to or inadvertent entry into stall, making recovery more difficult or impossible. The records include at least 3 crashes and 2 recovered LOC*

incidents involving stall and HST trim to the nose up stop. 2) It should be a certification requirement to provide envelope protection for backup or alternate FBW control law that do not meet CFR 25.173.
An overview of accidents on FBW-equipped airplane is presented in [8].

ALPA Assessment Hard and Soft Envelope Protection. Hard and Soft envelope protection evaluations conducted by ALPA on the A330 and the B777 pilot training simulators proved that the airplane with hard limiting could outperform the airplane with soft limiting, in contrast to the evaluators expectations **[4]** . The explanation is that for a design with hard envelope protection the pilot can simply pull the stick to the stop can and the computer will respond as fast as possible, in a safe/repeatable manner, to establish and track the NLF, AOA and Vmin limits, which come up in quick succession. It is very difficult or impossible for a pilot with average skills to do this manually with a system that uses soft protections. Generally there is no instrumentation to indicate the NLF, AOA limits, so it is impossible for pilots to quickly, safely and accurately approach them with such a system.

Still, "Hard Limiting" is not a panacea: the system must be available and failures in the hard envelope protection system can defeat this safety feature, witness the AF A330 Fl447 crash in the Mid-Atlantic Ocean and the A320 crash near Perpignan, France. These accidents dramatically illustrate that the introduction of envelope protection functions does not entirely do away with the LOC risk, because such systems also increase system complexity and the number of failure modes which introduce new real safety risks by themselves.

3 Envelope Protection Certification Requirements

General Systems-Related Certification Requirements

Both active and "Soft Envelope Protection" and "Hard Envelope Protection" control inceptor technology tend to have catastrophic failures modes that prevent continued safe flight and landing. Therefore both these designs rely on detection and isolation of the offending system component in a timely manner by the redundancy management system, using backup component and alternate (often simpler) control algorithms. For any system certification, including Envelope Protection, the designer must provide analyses and/or test data to demonstrate that the system meets the Code of Federal Regulations (CFR) safety requirements, in terms of function failure behavior and the crew's ability to cope with adverse operating conditions. CFR 25.1309 states: "The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane [must be] extremely Improbable" ($P<10^{-9}$ /flight hour), and the occurrence of any other failure condition which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions [must be] improbable" ($P<10^{-5}$ /flight hour). Also CFR 25.671 states "the airplane must be shown…to be capable of safe flight and landing for: …any combination of failures not shown to be extremely improbable…;…any jam encountered in the control position normally encountered unless shown to be extremely improbable.…" The interpretation by the applicant and the certification authorities is that these requirements can be met by providing failure detection, combined with alternate/back up means (modes) to assure continued safe flight and landing capability, to cover failure conditions that have a probability $P>10^{-9}$ /flight hour and that (without alternate or back-up means) would prevent continued safe flight and landing. This way, at least in the interpretation of the certification authorities, the pilots are provided with the ultimate control authority.

Clearly, operational safety for these complex designs hinges on the integrity (failure detection coverage, correct system reconfiguration and the pilot's ability to understand and cope with the complexities of the operating conditions encountered, including system reconfiguration and availability/status of protection functions.

Envelope Protection Certification Special Conditions

Important requirements paraphrased from Envelope Protection Special Conditions include:

General Limiting Requirements: envelope protection features must operate smoothly, be compatible with the airplane structural limits, allow for expected maneuvering considering margins to critical conditions and system tolerances. Dynamic characteristics, such as damping and overshoot, must satisfactory. Simultaneously engaged envelope limiting functions must not cause adverse coupling or adverse control priority.
Failure States: EFCS failures (including sensor) must not result in a condition where a parameter is limited to such a reduced value that safe and controllable maneuvering is no longer available. The crew must be alerted by suitable means if any change in envelope limiting or maneuverability is produced by single or multiple failures of the EFCS not shown to be extremely improbable.

Stall Protection.

a) Stalls must not be possible during pilot maneuvering, handling characteristics must be acceptable.

b) The airplane must be protected against stalls due to windshear and gusts at low speeds.

c) Accommodation of a reduction in stalling angle of attack due to icing conditions of Appendix C to 14 CFR part 25 must be verified.

d) System reliability and the effects of failures must be meet requirements of CFR § 25.1309.

e) The system must not impede pitch and speed control for any required maneuvering.

High Speed Protection. Operation of the high speed limiter during all routine and descent procedure flight must not impede normal attainment of speeds up to overspeed warning.

Normal load factor protection. In addition to the requirements of CFR 25.143(a) and in the absence of other limiting factors, the following apply:
1) The positive limiting load factor must not be less than:
   a) 2.5g for the EFCS normal state.
   b) 2.0g for the EFCS normal state with the high lift devices extended.
2) The negative limiting load factor must be equal to or more negative than:
   a) Minus 1.0g for the EFCS normal state.
   b) 0.0g for the EFCS normal state with high lift devices extended.

Pitch and Roll Angle Limiting. A margin in pitch control should be available to enable speed control in maneuvers such as climb after takeoff, and balked landing climb. The pitch limit should not impede likely maneuvering made necessary by collision avoidance efforts. A negative pitch limit should similarly not interfere with collision avoidance capability or with attaining and maintaining speeds near V_{MO}/M_{MO} for emergency descent.

Spiral stability, and the roll limit must not restrict attaining roll angles up to 65 degrees (approximately 2.4g level turn). The steady lateral control inceptor force to maintain a constant bank angle must not require excessive pilot strength as stated in CFR § 25.143(f).

In addition to CFR § 25.143, the following requirements apply:
The pitch and roll limiting functions must not restrict or prevent attaining roll angles up to 65 degrees or pitch attitudes necessary for emergency maneuvering. Spiral stability, which is introduced above XX degrees roll angle, must not require excessive pilot strength to achieve roll angles up to 65 degrees.

Additional EP Design Considerations and Guidelines. The author of this paper proposes the following additional Envelope Protection system design safety and performance guidelines. The system should

- engage and disengage without significant/objectionable airplane response transients
- not engage and interfere during normal vertical maneuvering with a normal load factor up to .2 and bank angles up to 35 degrees at an operating speed of 1.3Vstall-1g or higher

- not exhibit nuisance engagement interfering with normal control during conditions with moderate level of turbulence during operations at an airspeed 1.3Vstall-1g or higher
- not engage and latch as a result of a transient vertical or horizontal gust, resulting in a permanent change of the vertical control reference command or control mode
- exhibit an airspeed response damping coefficient equal to or greater than .7
- not exhibit an undershoot of Vmin and or overshoot of Vmax of more than 2% of min or Vmax during high rate EP entry maneuvers
- reach a speed within 10 % of the final stabilized Vmin or Vmax within 30 seconds after the pitch control effector reaches the stop
- limit the range of the reference speed command selection capability on the automatic flight Guidance and Control Mode Panel between 1.3 Vstall-1g and Vmo/Mmo
- not prevent immediate airplane response when the control effector deflection is reversed
- meet the above performance objectives without and with automatic thrust control engaged.
- not prevent the maximum safe Normal Load Factor to be established within 5 second after application of the full vertical control effector deflection. A NLF = 90 % of the limit structural or aerodynamic NLF , whichever is lower, is considered the maximum safe NLF
- prevent stall during combined high rate vertical and lateral maneuvering (large combined vertical and lateral inceptor deflections)
- be designed to assure that the aerodynamic or structural NLF-limit will not be exceeded for worst case (PIO) stop to stop reversals of the control inceptor deflection at any frequency of reversal and at any speed
- be designed and evaluated to assure satisfactorily low PIO susceptibility
- limit the NLF command for a full **nose down** vertical control effector deflection to $.5(1/\cos\varphi - 1)$, where φ is the roll angle. This approach eliminates the possibility of inadvertent negative load factor commands due to inadvertent stop to stop vertical control effector deflection (e.g. PIO). It also provides ample maneuver authority for collision avoidance and initiation of an emergency descent (see simulation results Figure 4.2 below)
- should adjust the NLF command structural limit by a factor equal to the ratio: (design weight for the structural NLF limit)/(the instantaneous airplane weight at any flight condition)
- limit the roll angle to 60 degrees in the opinion of the author, because there are few, if any, practical situations where a higher roll angle would gain a significant performance advantage, while the risk of LOC increases exponentially with increasing roll angle
- not impose an artificial pitch angle limit (in the opinion of the author), except to prevent tail strike during take off and landing. For all other cases artificial pitch angle limiting inevitably reduces the airplanes ultimate maneuver performance capability, which should be accessible for emergency collision or CFIT avoidance maneuvers. The airplane's ultimate maneuver performance is achieved when the NLF is at, or as near as safely possible to its aerodynamic or structural limit, whichever is smaller. This NLF-limit, together with the margin of airspeed above Vstall-1g, the AOAstall angle, the prevailing thrust/weight ratio and the prevailing horizontal and vertical wind condition determine the actual safe airplane flight path angle and pitch attitude limits.

4 Envelope Protection Design Concepts

Airspeed Envelope Protection

As discussed above, most stall, spin and overspeed accidents and incidents are attributed to flight crew errors in maintaining airspeed during manual control and partially automated control, even for cases where system failure played a role. Traditional autopilots and FBW control algorithms do not incorporate the necessary airplane performance information and or control priority logic to prevent airspeed divergence due vertical maneuvering without active thrust control. Even with the Autothrottle speed control engaged, the airspeed can diverge into LOC due to stall or overspeed, if the autopilot commands a climb or descent rate in excess of the airplane's steady state climb/descent capability at maximum or minimum thrust. Still, the unprotected autopilot vertical speed mode remains available on most transport airplanes. Until recently the

predominant emphasis has been on achieving error free pilot performance to detect and intervene when an unsafe airspeed condition develops. It is not surprising that this approach has met with limited success. An Envelope Protection approach relying solely on flight crew alerting is not likely to provide the desired level of protection. A better approach is to reduce the opportunities for "pilot error" by providing more effective pilot alerting during manual control and by the adoption of automatic control technology that prevents speed divergence outside the safe flight envelope. The necessary flight control technology has long been available, but the adoption has been very slow.

High Speed Protection. By necessity Mach or Calibrated Airspeed sensors must be used to provide automatic high speed protection and crew alerting. As an example, the TECS system uses one generalized airspeed control algorithm for all airspeed control functions. During automatic mode operations speed-on-elevator control priority is generally used as part of its basic MIMO control strategy, when the thrust command reaches the idle limit to control airspeed to the reference Mach or Calibrated Airspeed command, thereby eliminating the risk airspeed divergence and overspeed, without the need of a separate Vmax protection control algorithm. During augmented manual nose down "zoom" maneuvers a speed-on-elevator control priority is invoked when necessary to limit airspeed to Vmax.

For more traditional SISO-based automatic control systems a more or less conventional speed-on-elevator control algorithm with speed control priority can be added to the automatic control mode repertoire to provide the high speed protection.

As discussed above, a "Soft Envelope Protection" approach for new FBW airplanes is also possible.

For all types of high speed envelope protection it is necessary to provide proper flight crew alerting, to make them aware that the high speed envelope protection is in effect.

Airspeed-based Low Speed Protection. It is possible to provide low speed envelope protection using an airspeed control approach, analogous to high speed protection approach. This approach is used in the TECS design, where the Calibrated Airspeed and Mach sensors and control algorithm used for normal speed control are also used for the low speed protection function. As discussed above, TECS does not need or use explicit speed envelope protection for its automatic modes, because it is part of it basic control strategy.

The TECS augmented manual control mode is protected to allow "zoom" maneuvers by invoking a a speed-on-elevator control priority when necessary to limit airspeed to Vmin or Vmax. This approach is simple and effective, but relies on the simultaneous NLF control to prevent "dynamic stall". Therefore a full nose up vertical control effector deflection always commands the maximum allowable NLF for the instantaneous flight condition. This maximum allowable NLF is equal to the airplane NLF authority (determined by the aerodynamic or structural limit) minus a .1 safety margin, minus the NLF increment due to simultaneous lateral maneuvering. In this approach Vmin directly relates to Vstall-1g. The 1g stall speed is first calculated in terms of equivalent airspeed using the maximum lift coefficient for the existing airplane configuration and airplane weight and then converted into a true airspeed based 1g stall speed, for use in the Vmin protection control algorithm. The approach is analogous to the calculation of the Reference Speeds marked on the Primary Flight Display speed scale. Airplane weight can be derived from the take off weight on the airplane loading manifest, updated for the fuel burn. Alternatively and preferably, in-flight the airplane weight can be calculated with sufficient accuracy using measured AOA, the AOA-lift coefficient relationship, the measured dynamic pressure and the measured NLF. The resulting weight calculation can/should be correlated further to the weight calculated by the first method.

TECS Augmented Manual Mode – High/Low Speed Protection

For the FBW manual control on commercial transport airplanes, a design allowing "Carefree Maneuvering" to the absolute limits of the safe airplane performance capability is desirable. In other words, the only limitation placed on manual maneuvering is to avoid stall, keep the Normal Load Factor within the

aerodynamic/structural limits and keep the roll angle and sideslip within the demonstrated safe capability. Thus, it should be possible to operate safely with and without automatic thrust control and execute "zoom" maneuvers taking the airplane outside the airplane's constant speed performance capability, assuming the airplane is at a high enough altitude to avoid terrain and ground obstacles. This approach was pursued for the TECS/THCS technology demonstration system. It uses the TECS Core Control algorithm, which is shared with the automatic control modes, to provide an augmented manual Flight Path Angle Rate Command/Hold (FPARCH) control mode with "Direct Manual FPA Control" capability. It can be operated safely to the limits of the airplane performance capability, with the Autothrust ON, or OFF, by the incorporation of Vmin and Vmax speed envelope protection, thereby achieving an "Equivalent Level of Safety" required for certification. The details of this design are described in [9, 10, 11].

For speed envelope protection, separate normalized a longitudinal acceleration error control signals ($\dot{V}_\varepsilon / g$) are computed with respect $V_{\min}$ and $V_{\max}$. The speed envelope limits $V_{\min}$ and $V_{\max}$ are defined differently for the Autothrust ON and OFF cases. The augmented manual mode vertical maneuvering is controlled by a the flight path angle error signal (γ_ε), which can be used interchanged with $\dot{V}_\varepsilon / g$ error signal to prioritize $V_{\min}$ and $V_{\max}$ speed-on-elevator control.

When the autothrust is engaged, the $V_{\min}$ control function is armed to allow engagement after the thrust-command reaches Tmax and after the $V_{\min}$ control develops a $\dot{V}_\varepsilon / g$ signal that produces an elevator command that is more nose down than the γ_ε control signal developed by the manual flight path angle control. Similarly, the $V_{\max}$ control function is armed to allow engagement after the thrust-command reaches Tmin and after the $V_{\min}$ -control develops a $\dot{V}_\varepsilon / g$ signal that produces a more nose up elevator command than the γ_ε signal produced by the manual flight path angle control. This logic is used with Autothrust is ON or OFF.

For the Autothrust ON case, $V_{\min}$ is defined as $V_{\min} = V_{cmd} - \delta_{vci}.(V_{cmd} - 1.05V_{stall_\varphi})$, wherein V_{cmd} is the normal automatic speed control mode speed command, V_{stall_φ} is the stall speed at a bank angle φ, defined as $V_{stall_\varphi} = V_{stall1g}\sqrt{1/\cos\varphi}$, $V_{stall1g}$ is the 1g stall speed and δ_{vci} is the vertical control inceptor deflection. The full vertical control inceptor deflection is normalized to +1,-1. When the inceptor is held at a constant nose up deflection, the γ_{cmd} will continue to rise after Tmax is reached and the speed will start to bleed off. Then, after the $V_{\min}$ -protection control priority is invoked the deceleration will be arrested, to stabilize the speed at $V_{\min}$. For a sustained full nose up inceptor deflection the speed will bleed off to $V_{\min} = 1.05\, V_{stall1g}$ and when the inceptor is released, the speed will return to the pilot selected V_{cmd} on the MCP. For sustained partial nose up inceptor command the speed will end up part way between V_{cmd} and $V_{\min}$. The stall speed is defined in terms of equivalent airspeed because the so defined stall speed does not vary with altitude. Within the speed control algorithm equivalent and indicated airspeeds and commands are converted to true airspeed to compute the Vdot-error/g signal. Similarly, for $V_{\max}$ protection with Autothrust ON, $V_{\max}$ is defined as $V_{\max} = V_{cmd} - \delta_{vci}.(V_{Vmo/Mmo} + K_{V_{\max}} - V_{cmd})$. So for sustained full nose down stick command the airspeed ends up at $V_{\max} = V_{cmd} + K_{V_{\max}}$ and when the inceptor is returned to zero deflection the

airspeed returns to V_{cmd}. The constant $K_{V_{\max}}$ should be selected to assure safe operation during a manual emergency descent maneuver with the inceptor defected full nose down, e.g. allowing a speed close to V_D. For sustained partial nose down stick command the speed will end up part way between V_{cmd} and $V_{\max}$.

For the Autothrust OFF case, the $V_{\min}$ / $V_{\max}$ protection is always armed. In this case there is no V_{cmd} and $V_{\min}$ is defined as $V_{\min} = K_{V_{\min}}.V_{stall_\varphi} - \delta_{vci}.(K_{V_{\min}} - 1.05).V_{stall_\varphi}$. Therefore the speed is allowed to bleed off from the speed at the start of the vertical maneuver until the $V_{\min}$-protection is invoked to halt the deceleration and stabilize the final speed at $V_{\min}$. For a sustained full nose down inceptor deflection the speed will end up at $V_{\min} = 1.05.V_{stall_\varphi}$. Then when the inceptor is returned to zero deflection the speed returns to $V_{\min} = K_{V_{\min}}.V_{stall_\varphi}$. The factor $K_{V_{\min}}$ should be selected to assure the speed returns at a minimum safe operating speed, after the pilot returns the inceptor to neutral, e.g. $1.2V_{stall_\varphi}$. For sustained partial nose down stick command the speed will end up part way between $K_{V_{\min}}.V_{stall}$ and $V_{\min} = 1.05V_{stall_\varphi}$. Similarly, for $V_{\max}$ protection with Autothrust OFF, the $V_{\max}$ is defined as $V_{\max} = V_{Vmo/Mmo} - \delta_{vci}.K_{V_{\max}}$. So for sustained full nose down inceptor command the airspeed ends up at $V_{Vmo/Mmo} + K_{V_{\max}}$ and when the pilot returns the inceptor to neutral the speed will return to $V_{Vmo/Mmo}$. For a sustained partial nose down inceptor command the speed will end up part way between $V_{Vmo/Mmo}$ and $V_{Vmo/Mmo} + K_{V_{\max}}$.

This way a pseudo speed stability is established after the $V_{\min}$ or $V_{\max}$ control priority is invoked and the final speed deviation will be proportional to the stick deflection. This concept is compatible with CFR 25.173 for speed stability.

Airspeed-based Vmin Protection Simulation Results. Figure 4.1 shows the aircraft responses for the Autothrust ON case (left plot) and for the Autothrust OFF case (right plot), for a .1 unit nose up inceptor command at t=10 seconds and maintained indefinitely. The initial condition IAS_{cmd}=250 Knots, Altitude H =10,000 ft. The speeds are recorded in equivalent airspeed.

For this case the inceptor commands a constant rate of change Flight Path Angle (for this speed equivalent to Δn_z = ~.1) until the $V_{\min}$ control priority is invoked, at which time the $V_{\min}$ control captures and stabilizes the airspeed at $V_{\min}$. When the $V_{\min}$ control priority is invoked the γ_{cmd} is synchronized with the actual γ, so the two response traces merge. Switchover to $V_{\min}$ control priority is always transient free, because the feedback control for γ and longitudinal acceleration are fully normalized (exhibiting the same dynamics) and takes place when the error signals cross over in amplitude. Furthermore, error switching takes place upstream of the Core Controller integral control signal path.

With the Autothrust ON, the $V_{\min}$ control cannot engage until the thrust command has reached Tmax. The final speed is $V_{\min} = V_{cmd} - \delta_{vci}.(V_{cmd} - 1.05V_{stall_\varphi})$. So for this case with $\delta_{vci} = .1$ unit, only 10 % of the speed margin is used and final speed ends up only about 9 knots below the pilot selected V_{cmd}

on the Mode Control Panel. The final γ is the γ at max thrust, at $V_{\min}$. The maximum available thrust is falling off with increasing altitude, therefore the γ also keeps falling off.

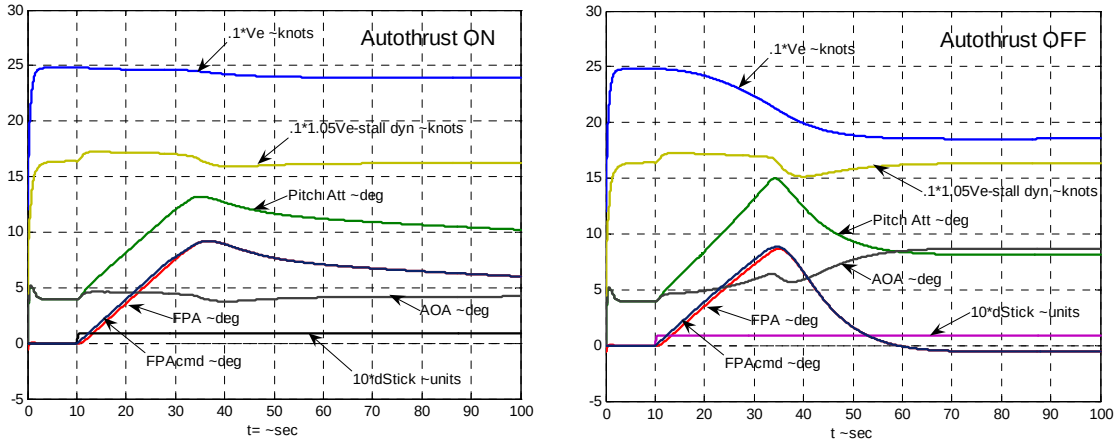

Figure 4.1. Speed Envelope Protection: Airplane responses for .1unit NU Stick input, starting at maneuver speed V_{IAS}=250 Knots, Altitude =10,000 ft

For the Autothrust OFF case, $V_{\min} = (1.2 - .15\delta_{vci}).V_{stall_\varphi}$, assuming $K_{V_{\min}} = 1.2$, so in this case the airspeed settles at a $V_{\min}$ which is slightly below $1.2V_{stall_\varphi}$ and the final settles at a slightly negative value, because at $V_{\min}$ the airplane is on the backside of the Speed-Drag curve, so drag has increased.

Figure 4.2 shows the aircraft responses for the Autothrust ON case (left plot) and for the Autothrust OFF case (right plot), for full nose up inceptor command at t=10 seconds and after stabilization at $V_{\min}$, a full nose down (-1 unit) inceptor command starting at t=55 seconds, allowing the airplane to stabilize at $V_{\max}$. The initial condition was IAS_{cmd}=250 knots, altitude H = 10000 ft. The speeds are recorded in equivalent airspeed; V_{mo} = 375 knots, $K_{V_{\max}}$ = 25 Knots, therefore for full nose down inceptor $V_{\max}$=400 knots; $V_{stall1g}$=156.2 knots, the AOA_{stall} = 15 degrees. The Envelope Protection engagement is recognizable at the point where the γ_{cmd} starts to synchronize with the actual γ.

For the Authrust ON case, the maximum γ achieved for the full nose up stick maneuver is ~25 degrees, the maximum pitch attitude is ~31 degrees. For the Autothrust OFF case the maximum achieved FPA is ~18 degrees and the maximum pitch attitude is ~24 degrees. For both the autothrust ON and OFF cases the maximum NLF (not shown) achieved is ≈2.4, which is close to the theoretical safe limit at the maneuver speed V_{IAS}=250 Knots. This is also borne out by the plotted variable $1.05V_{stall-dyn}$, which reaches a value equal to the actual airspeed speed shortly after the full nose up command initiation.

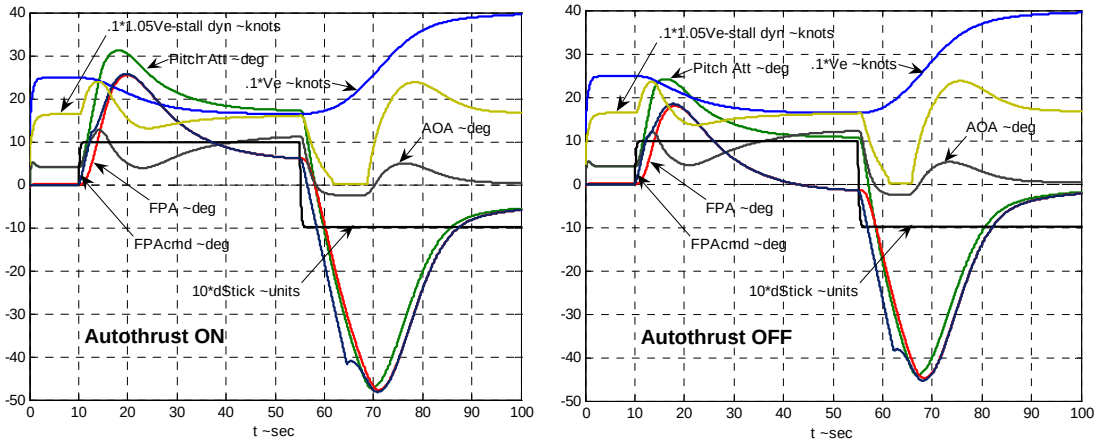

Figure 4.2. Speed Envelope Protection: Airplane responses for Full NU and ND stick inputs, starting at maneuver speed V_{IAS}=250 Knots, Altitude =10,000 ft

It then drops well below it, because a well damped/undershoot free capture of $V_{\min}$ requires a reversal of the NLF, which reduces $V_{stall-dyn}$. Finally the airspeed settles $1.05\,V_{stall-dyn} = 1.05\,V_{stall\,1g}$, since $\varphi = 0$. The temporary NLF reversal also causes a temporary drop in the AOA response below the AOA safety limit, which for a full nose up stick input corresponds to ~.9 $C_{L_{\max}}$. Here $C_{L_{\max}}$ =1.5 at AOA_{stall} =15 degrees and .9 $C_{L_{\max}}$ occurs at AOA= 12 degrees. So, for this extreme maneuver with the stick held at the full nose up deflection, the AOA should not exceed 12 degrees, either dynamically or in the final steady state condition with $V = V_{\min}$. The $V_{\min}$ -based stall protection shown here meets this requirement.

An important conclusion is that it is not possible to achieve a well damped capture of $V_{\min}$ *while holding the AOA at the allowed static AOA limit.* The full nose down stick maneuver from $V_{\min}$ to $V_{\max}$, starting at t=55 seconds is the most extreme vertical maneuver possible. The $V_{\min}$ and $V_{\max}$ control computations are the same as for normal speed control, except the V_{cmd} is replaced with respectively $V_{\min}$ or $V_{\max}$, computed separately for Autothrust ON and for Autothrust OFF, as described above. For the nose down command the lowest normal load factor achieved is 0 absolute (Δn_z = -1), recognizable by the AOA is staying constant at -2 degrees (Lift Coefficient = 0, n_z =0), for a short duration just prior to achieving the most negative γ. *The most negative FPA and pitch attitude achieved during this extreme nose down maneuver are between -43 and -47 degrees. This provides ample evidence that allowing a more negative normal load factor, e.g.* n_z *=-1, is completely unnecessary, unless flying upside down!* Limiting the nose down Δn_z to -1 also provides additional protection against the potential severity of the responses in case of a PIO, which can never be ruled out entirely.

Another not so intuitive design requirement is related to disengagement of the airspeed envelope protection function: these functions must remain engaged as long as the main vertical maneuver control algorithm produces a pitch command that is opposite to, or in the same direction but smaller in magnitude than the EP command. The magnitude of the EP command is an indication of the urgency (rate) of EP maneuvering needed to arrest the rate of speed change to prevent "blowing" through the limit, so it should not be replaced by a lower command from the main vertical maneuver control algorithm, even if that command has a the same sign. This situation occurs, for example, during a hard pull up by the pilot, when the high rate of airspeed fall off may trigger the pilot to back off and slightly reverse his input.

Still another Envelope Protection requirement is illustrated on figure 4.3.

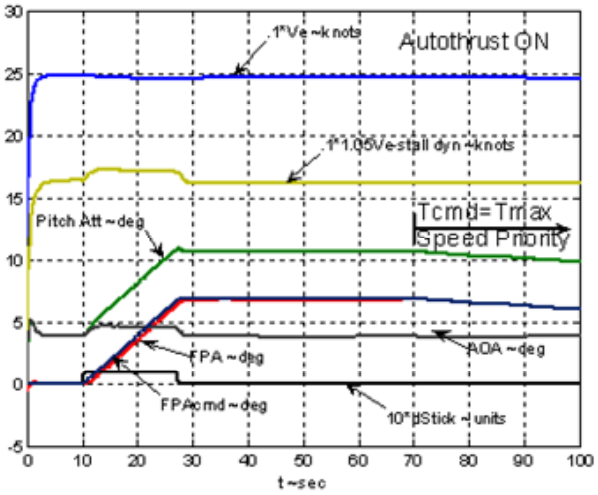

Figure 4.3 Envelope Protection: Transition to Speed Control Priority during climb at constant FPA

During FBW manual control operation with the Autothrust ON, the pilot may establish a γ_{cmd} that requires a thrust close to Tmax or Tmin. Then, due to the engine lapse rate with changing altitude the thrust command may reach Tmax or Tmin. At that point then speed control priority must be invoked to maintain the V_{cmd} selected by the pilot on the Mode Control Panel, otherwise the airspeed will start to run away, first slowly, then faster and faster, as the actual thrust deviates more and more from the thrust required for the established γ_{cmd}. In figure 4.3 this reversion to speed control priority occurs at t = 70 seconds.

AOA-based Stall Protection

Angle of Attack can be used in several ways to provide stall protection. The most direct approach is to select an AOA_{lim} and design an independent AOA control algorithm that will control the airplane to this AOA_{lim}, using the elevator. Design issues associated with this approach include

- inherent lack of airspeed response damping when controlling strictly to AOA (undamped phugoid oscillation, excited by stick input commanding a change in AOA)
- selection of the AOA_{limit}, appropriate for pilot-in-the-loop maneuvering and for steady state conditions with the stick at neutral, particularly at low speeds
- AOA_{lim}-control engage and disengage logic
- AOA sensor calibration, as a function of flight condition and for the effects of sideslip angle
- effect of vertical maneuvering on the accuracy of sensed AOA (flow field effects, effect of moment arm between sensor location and the airplane center of gravity)
- AOA sensor reliability and availability. Traditionally, AOA sensors have not been considered reliable enough for use in flight critical applications. AOA-vanes or pressure probes are subject to icing and mechanical damage that may affect their accuracy and reliability.

All of these issues must be dealt with to achieve a satisfactory design. Here, we shall only discuss the first three issues.

The natural airplane Phugoid mode is characterized by very lowly damped airspeed and altitude fluctuations that ~180 out of phase and the airplane Total Energy staying nearly constant. Therefore a pure AOA control algorithm using the elevator is unacceptable, because it does not provide adequate airspeed,

altitude and NLF response damping. Artificial airspeed damping must be provided and the damping coefficient should be $\geq .7$. This can be achieved by adding vertical speed, flight path angle, or longitudinal acceleration (rate of change of airspeed) feedback to the AOA control. For a system with less damping the response to a sudden full nose up command from an initial airspeed $\geq 1.V_{stall}$ will be an unacceptable undershoot of $V_{stall1g}$ and a continued airspeed , flight path and NLF oscillation. A pilot holding the stick at the stop to get max performance cannot damp that oscillation. However, the consequence of adding airspeed/vertical path damping is that the AOA will drop temporarily below the AOA_{limit} and then slowly return to the AOA_{lim}, as the airspeed approaches the steady state condition, as shown in figures 4.2.

A reasonable baseline value for the AOA_{lim} is a value AOA_{Ref} achieved during 1g flight at ~1.2 $V_{stall1g}$ (pilot out of the pitch control loop), considering that the Envelope protection functions should not interfere with normal vertical and lateral maneuvering at the lowest operational airspeed. The maximum safe and achievable AOA, defined as AOA_{max}, for full nose up stick maneuver conditions should yield ~$.9\,C_{L_{max}}$ when $AOA=AOA_{max}$ and this AOA_{max} corresponds to 1g flight at ~$1.05\,V_{stall1g}$. For the simulation used here, $.9\,C_{L_{max}}$ occurs at AOA_{max} = ~12 degrees. *This way Envelope Protection incurs no performance penalty, because the airspeed should never be allowed to go below* $1.05\,V_{stall1g}$.

The AOA_{lim} , modulated as a function of inceptor input, becomes: $AOA_{lim} = AOA_{ref} + \delta_{vci}.(AOA_{max} - AOA_{ref})$. Using this approach the following AOA-based equivalent $(\dot{V}_\varepsilon / g)_{AOA\text{-}based}$ control signal was defined and used to generate the simulation results shown in Figure 4.5 and 4.6: $(\dot{V}_\varepsilon / g)_{AOA\text{-}based} = -[AOA_{ref} + \delta_{vci}.(AOA_{max} - AOA_{ref}) - AOA_{filtered}] - K_{Vdot}.(\hat{\dot{V}} / g) + K_{AOAdot}.(AOAdot)_{derived}$. The $K_{Vdot}.(\hat{\dot{V}} / g)$ term provides the airspeed and flight path response damping, the $K_{AOAdot}.(AOAdot)_{derived}$ term helps to smooth out the engage transient. The $AOA_{filtered}$ signal is derived in a bias-compensated second order AOA-filter, using $(AOAdot)_{inertial}$ as defined by the Euler equation of motion along the airplane Z-axis. The $\hat{\dot{V}} / g$ signal is similarly derived in a bias-compensated first order Airspeed/Groundspeed filter or a second order Airspeed/longitudinal acceleration filter and this signal is also used for all other speed control functions. It should also be noted that the $(\dot{V}_\varepsilon / g)_{AOA\text{-}based}$ signal is used in an integral control signal path, so that the term $K_{AOAdot}.(AOAdot)_{derived}$ into the integral control signal path is equivalent to using $K_{AOAdot}.(AOA)_{filtered}$ term in a proportional control signal path. Control priority is invoked to replace the γ_ε signal input to the elevator control when the $(\dot{V}_\varepsilon / g)_{AOA\text{-}based}$ signal produces a command that is more nose down than the γ_ε signal.

In figure 4.4 the airplane responses for this AOA-based stall/low speed protection function are shown for a full nose up stick command at a trim condition with IAS=250 knots, H =10,000ft, for cases with Autothrust ON and OFF. It may be observed that for Autothrust ON case, the initial peak AOA response does not quite reach the AOA_{max} = ~12 degrees and then falls back as low as 5 degrees, before it slowly approaches and settles at AOA_{max}. The AOA-control engagement occurs very soon after the full nose up stick is applied and causes a hick-up in the pitch attitude response. For Autothrust OFF case, the AOA control engages immediately after the inceptor input is applied, causing the γ_{cmd} to synchronize to γ. The initial peak AOA response remains far below the AOA_{max} = ~12 degrees, falls back less (again to ~5 degrees) and then rises slowly to AOA_{max} with a slight overshoot. The long term airspeed response appears over-damped and somewhat sluggish, but the airspeed settles on a value ~$1.05\,V_{stall_\varphi}$ without an undershoot (here $\varphi = 0$). It is clear that especially the Autothrust OFF cases does not achieve the full airplane n_z-performance capability in terms of reaching AOA_{max} during the early part of the maneuver.

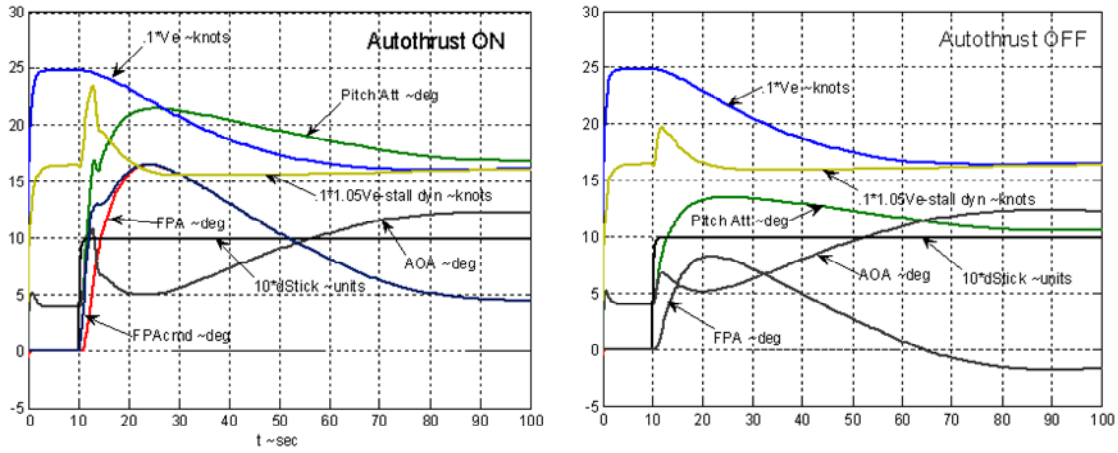

Figure 4.4 AOA-based Stall/Low Speed Protection. Responses for Full NU stick at IAS=250 knots

Likewise, the airplane responses for the same extreme vertical maneuver, starting from IAS =1.2 $V_{stall1g}$ were also found to not achieve the full AOA_{max} performance potential for the Autothrust OFF case. The author briefly attempted to remedy the noted deficiencies of the direct AOA control based stall and low speed EP approach, but it soon became clear that the AOA-based design would require a lot of flight condition dependent customization. ***The conclusion is: inordinate design complexity can be avoided by utilizing a generalized control strategy that can seamlessly accommodate all needed modes of operation, without requiring a significant amount of customization for each sub-function. This approach provides operational performance consistency between modes and reduces the required number of sensors and laboratory and flight test development assurance efforts.***

Stall Protection using AOA derived V_{min}.

Still another way to provide Stall/Low Speed Protection is to use the defined AOA_{lim} to derive the corresponding 1g V_{min} and then use the same V_{min} -based stall protection control as used above. This approach is based on using the 1g relationship between airspeed and AOA. For a constant speed 1g condition the relationship between airspeed and AOA is $dV_{true}/d\alpha = -.5V_{true}.C_{L_\alpha}/C_{L_0}$, where α =AOA is the angle of attack, C_{L_α} is the lift slope gradient at an AOA corresponding to 1g flight at V_{true} and $C_{L_0} = W/(\bar{q}.S)$. Here W and $\bar{q}$ are the instantaneous airplane weight and dynamic pressure. Then the airspeed error relative to the 1g V_{min} that corresponds to the AOA_{lim} is $(V_{true})_\varepsilon = -.5V_{true}.(C_{L_\alpha}/C_{L_0}).\alpha_\varepsilon$, where α_ε is the angle of attack error relative to the reference AOA_{lim}. Since the lift curve slope in the vicinity of AOA_{lim} is likely to be non-linear, the calculation of $(V_{true})_\varepsilon$ may be in error at speeds away for the reference 1g V_{min} and AOA_{lim}. This effect is mitigated by using the so derived airspeed error only for low frequency control. Therefore this airspeed error is processed through a first order lag function and the resulting lagged airspeed error signal is complemented (lag-compensated) by adding a washed out true speed signal to it, to provide a robust V_{min} control error signal. The lag and the washout use the same ~10 second time constant.

Figure 4.5 shows the airplane responses for a full nose up stick command starting at IAS= 200 knots and

H =10000 ft, using this approach to Stall/$V_{\min}$ protection. These responses are quite satisfactory and nearly the same for both the Autothrust ON and OFF cases.

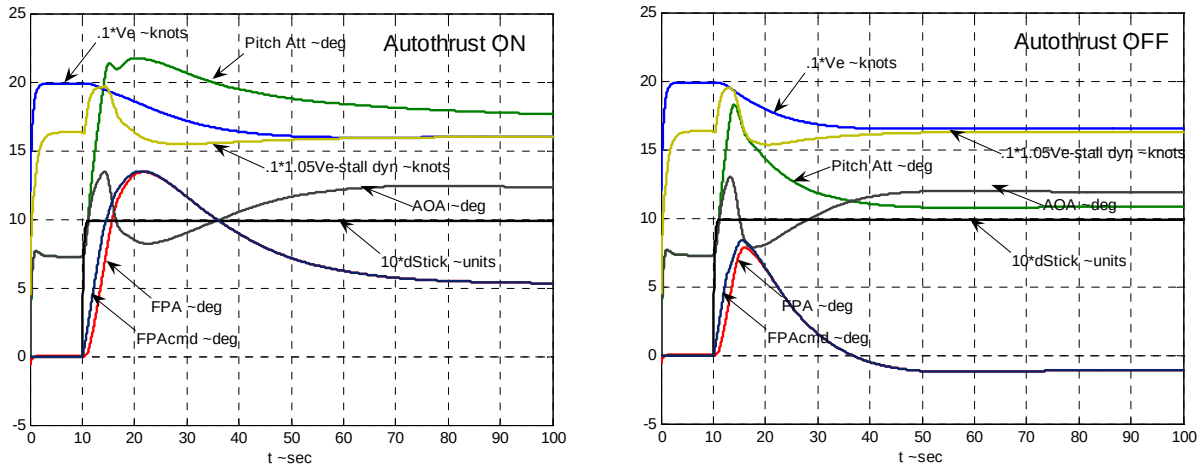

Figure 4.5 Stall Protection using AOA derived V_{min}. Responses to full nose up stick, IAS =200 knots

For the Autothrust ON case there is a slight pitch attitude bobble when the EP engages, but this is not a significant issue, considering this extreme full nose up stick maneuver. Here $V_{stall_\varphi} = V_{stall1g}$, since $\varphi = 0$ and after t=~50 seconds $V_{stall-dyn} = V_{stall1g}$. The momentary exceedance of the AOA_{max} (=12 degrees) is acceptable as long as it can be ascertained that the AOA_{stall} will never be exceeded.

Normal Load factor Protection.

As alluded to above, the primary method of Normal Load Factor protection is to limit the n_z commanded by a full nose up or nose down vertical control inceptor (δ_{vci}) deflection to the available n_z-vertical authority, which may to be adjusted for the Δn_z required for a coordinated turn, as discussed in the next section. However, depending on the design, this approach may provide adequate protection for stop to stop δ_{vci} inputs, e.g. due to an inadvertent PIO at high speed and a separate innerloop n_z-limit feedback controller may be needed.

Roll Angle Protection

The relationship between Normal Load Factor (n_z)and roll angle (φ) in a coordinated level turn at constant roll angle is $n_z = -A_z / g \approx 1/\cos\varphi$, where A_z is the output of an accelerometer aligned with the airplane z-body axis (positive down). As a result the stall speed in a coordinated level turn is $V_{stall\varphi} \approx V_{stall1g}\sqrt{1/\cos\varphi}$. For example, for φ =25 degrees n_z = ~1.1, therefore $V_{stall25}$ = ~ $1.05\,V_{stall1g}$. Likewise, at $\varphi = 60$ degrees $n_z = \sim 2.0$ and $V_{stall60} = \sim 1.414\,V_{stall1g}$. Recall that the nose up NLF-authority is $(n_z)_{\text{authority}} = V^2/V^2_{stall1g}$, therefore the available the nose up vertical maneuvering

authority in a bank angle is $(\Delta n_z)_{\text{NUauth}}=(V^2/V^2_{stall1g}\text{-}1/\cos\varphi\text{-}.1)$. If a 30 degree bank angle capability is desired at $V=1.2V_{stall1g}$ and a safety margin Δn_z = .1 is maintained, then it follows that $(\Delta n_z)_{\text{NUauth}}=[(1.2V_{stall1g})^2/V^2_{stall1g}\text{-}.1\text{-}1/\cos 30]=.185$, which is adequate for gentle vertical flight maneuvering. Then, if the same vertical maneuver authority is reserved at all speeds $V\geq 1.2V_{stall1g}$, the remaining NLF authority can be used for roll maneuvering and the resulting at a given airspeed and airplane configuration can be calculated from the equation $\varphi_{\text{lim}}=\cos^{-1}[1/(V^2/V^2_{stall1g}\text{-}.285)]$. Using this approach, φ_{lim} will always occur at the same AOA for a given airplane configuration. This equation yields φ_{lim}=30 degrees at $V=1.2V_{stall1g}$, φ_{lim} = ~44.6 degrees at $V=1.3V_{stall1g}$, φ_{lim} = ~53.3 degrees at $V=1.4V_{stall1g}$, and φ_{lim} = ~60 degrees for $V=1.51V_{stall1g}$. In this study the a minimum value of φ_{lim} = 25 degrees was mained for speeds $V\leq 1.18V_{stall1g}$ where this limit is first encountered. The above described V_{min} based stall and low speed protection used the above defined $V_{stall\varphi}$ to compute the target V_{min} as a function of the bank angle and vertical control stick deflection.

Figure 4.6 shows the roll angle response to a full lateral control inceptor deflection ($\delta_{lci}=1$) and zero vertical control inceptor deflection ($\delta_{vci}=0$) for various values of $V/V_{stall1g}$, using the above strategy of maintaining a constant vertical maneuver margin at φ_{lim}. The plot was generated using the Roll Rate Command/ Roll Attitude Hold Control mode of the generalized/integrated THCS lateral directional control demonstration system. In this design the lateral control inceptor commands a roll rate and for $\delta_{lci}=0$ the established roll will be maintained if $\varphi\leq 30$ degrees. When the lateral control inceptor is released at roll angles greater that 30 degrees (here at t=50 second), the roll angle decays back to 30 degrees, as seen in the plot, simulating a relatively high level of spiral stability.

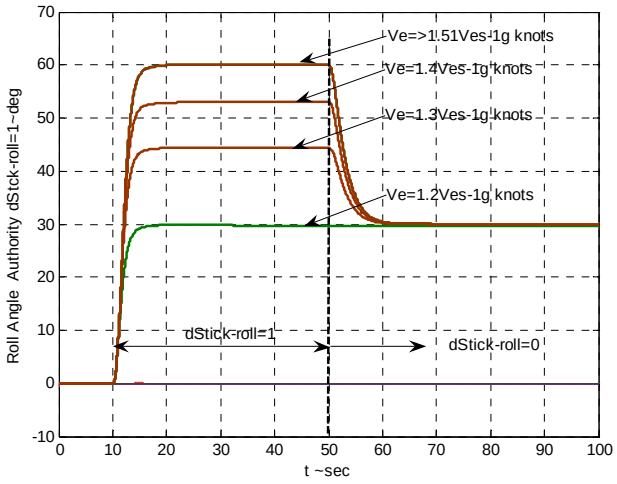

Figure 4.6 Roll angle authority φ_{lim} as a function of $V/V_{stall1g}$ at $\delta_{vci}=0$

In Figure 4.7 the roll angle responses are shown for various deflections of δ_{lci} at IAS=250knots, with $\delta_{vci} = 0$, to illustrate the maximum achievable roll angle as a function of δ_{lci} at this speed. This demo system was designed such that it always requires the same δ_{lci} deflection to achieve a given target bank angle above 30 degrees at any speed. The roll angle limit at full δ_{lci} is deliberately chosen on the high side to allow ample roll angle capability at any speed, while reserving only a relatively small amount of the NLF authority for gentle vertical maneuvering, without the need to first reduce the roll angle. Pilots do not use roll angles in excess of 30 degrees for normal commercial airplane operations and the airplane's safe NLF

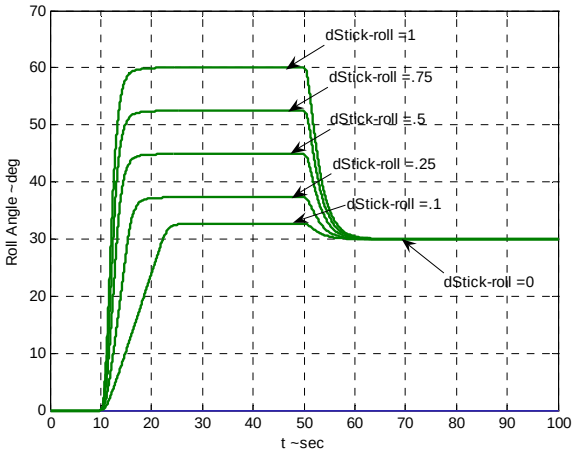

Figure 4.9 Roll Angle Responses for various δ_{lci} deflections, $\delta_{vci} = 0$, IAS =250 knots

capability not used for roll maneuvering remains available for immediately vertical maneuvering. Thus, to a large extend the pilot still retains the ability to allocate the available NLF authority between vertical and lateral maneuvering. However, for this design a deliberate negative Δn_z commanded by a nose down δ_{vci} deflection does not increase the computed roll angle authority limit ($\varphi_{\lim}$). For a design using direct and independent AOA control for stall protection there is in principle no need to provide roll angle limit protection, because stall at lower speeds due to excessive bank angle is prevented by invoking AOA_{limit} control priority, which will simply lower the nose as necessary to prevent stall as the bank angle is increased. This characteristic is different is different than the behavior of the design decribed above.

5 Conclusions

There is no doubt that the incorporation of Envelope Protection functions will help prevent accidents and incidents due to deficiencies in the current generation FG&C systems, as well as due to pilot error. At the earliest opportunity new airplanes should incorporate simpler, more generalized MIMO-based FG&C systems that can provide better integration of automatic and FBW augmented manual control, requiring fewer modes, fewer degraded backup control laws and fewer sensors that can fail. For normal (no fault) operations, the automatic modes of such designs can be fully protected against LOC without the need for explicit envelope protection functions, while EP for the manual control mode can be provided with little extra complexity. Envelope protection for airplanes with legacy FG&C systems can be provided as add-on functionality, but the design development will be more challenging and the resulting final design will significantly increase the overall FG&C system and operational complexity. Some new EP related mishaps must be expected, but overall, the application of Envelope Protection functions will save lives.

The overarching objective should be to continue development of simpler, more flight crew friendly FG&C systems, using less hardware that can fail (sensors, computers and interfaces), using more standardized/generalized and reusable functionality that over time leaves fewer development assurance flaws and reduces reliance on degraded backup up modes that present an underestimated risk of catastrophic "flight crew errors".

6 References

1. A.A. Lambregts, G. Nesemeier, J.E. Wilborn, and R.L. Newman, "Airplane upsets: Old problem, New Issues", AIAA paper 2009-6867

2. Richard L. Newman, "Thirty Years of Airline Loss of Control Mishaps", AIAA 2012-4495

3. "General Aviation Accident Prevention – Basic Envelope Protection; Phase III: Flight Test Results and Recommendations for Future Envelope Protection Systems" – DOT/FAA/AR-xx/xx; Sensis Report 201212371-01(draft final report),7 November 2012

4. Ron Rogers, "Pilot Authority and Aircraft Protections", ALPA/IFALPA publication, May 2001

5. "Requirements Regarding Pilot Authority and Flight Control Architecture", IFALPA aircraft Design and Operation Briefing Leaflet

6. "Accident of Airbus A-320-214, registration EC-HKJ, at Bibao Airport on 7 February 2001", Technical Report A-006/2001, Spanish Commission for Investigation of Accident and Incidents of Civil Airplanes (CIAIAC)

7. "Proximity incident between this Airbus A340 and A330 on 2000-10-02", Aircraft Accident Investigation Board (AAIB), United Kingdom

8. R. L. Newman, and A. A. Lambregts, "A Review of Fly-by-Wire Accidents", International Society of Air Safety Investigators; 40th Annual Seminar "Accident Prevention Beyond Investigations

9. A.A. Lambregts: Vertical Flight Path and speed Control Autopilot design Using Total Energy principles, AIAA 83-2239CP

10. A.A. Lambregts:Automatic Flight Controls Concepts and methods; Koninklijke Nederlandse Vereniging voor Luchtvaart, Jaarverslag, 1996

11. A.A. Lambregts: TECS Generalized Airplane Control System Design – An Update; 2013 CEAS conference on Guidance, Navigation and Control, Delft, The Netherlands