

CHAPTER 3
AIRWORTHINESS STANDARDS
TRANSPORT CATEGORY ROTORCRAFT

MISCELLANEOUS GUIDANCE (MG)

AC 29 MG 17. ROTORCRAFT ADVANCED FLIGHT CONTROLS (AFC).

a. Explanation.

(1) Introduction.

State-of-the-art flight control technology has outpaced previously provided guidance material. Technological advances in electronic systems make it feasible to employ advanced flight control systems for many functions that were previously implemented in part, or totally, by mechanical means. Advanced Flight Control systems are characterized by electronic primary flight controls and sophisticated control law implementation. These control law implementations can reduce pilot workload and enhance aircraft performance, but there are new considerations for showing compliance to flight rules. Application of previous guidance material may not be adequate to address advanced control laws, evidenced by maneuver demand controls, envelope limiting, and use of small displacement multi-axis controllers.

Efficient implementation of advanced systems may result in multiple functions being provided by a single type of system (if redundancy is not considered another system). These types of configurations are commonly referred to as “integrated systems.” Electronic/software implementations of integrated functions present new safety concerns. Failures associated with the layers of redundancy and possible resultant degraded modes of operation require additional considerations to ensure safety. Application of previous guidance material may not be adequate to address implementation of these integrated systems.

(2) Scope.

Mandatory terms used in this AC, such as “must”, are terms used only in the sense of ensuring the applicability of these particular methods of compliance when the acceptable means of compliance described herein are used. This AC does not change regulatory requirements and does not authorize changes in, or deviations from regulatory requirements. This AC establishes an acceptable means, but not the only means, of certifying rotorcraft Advanced Flight Control Systems.

The guidance contained in this document addresses areas that need special attention in the development and certification of Advanced Flight Control Systems installed and used on rotorcraft.

The term “Advanced Flight Controls” (AFC) is used to describe systems that differ from conventional flight control systems with respect to the applied signal processing and signal transmission technology. Conventional flight control systems typically use mechanical elements (rods, bell cranks) for transmitting command inputs from the pilot’s controls to the rotor blades for primary control. Conventional systems may include electronic stability augmentation systems and autopilots with limited authority that are superimposed on a mechanical primary flight control system. AFC systems, on the other hand, typically feature electronic signal processing and signal transmission using electrical wires (Fly-by-Wire), optical fibers (Fly-by-Light), or potentially even non-mechanical media (e.g., radio frequency control). Additional considerations are often introduced by novel forms of these types of flight controls systems implementations including, for example, unique control inceptors (e.g., side stick controllers) and/or control laws. Since AFC systems typically employ a high level of integration and increased functionality relative to conventional systems, greater possibility exists for failures that are not as obvious or testable as those for conventional flight control systems. Thus, AFC systems demand a higher integrity level to achieve the same safety level as existing mechanical systems; therefore, specific guidance is required for AFC systems. Furthermore, Special Conditions may be required to account for these novel characteristics to ensure that there is no degradation of safety. Additionally, this Miscellaneous Guidance (MG) will identify areas where special conditions/rule changes may be needed and where existing guidance may not be adequate.

Guidance material herein makes no distinction between normal/small and transport/large category rotorcraft employing AFC systems. This guidance primarily concentrates on FAR Part 29 applications; however, this guidance is applicable to FAR Part 27 AFC applications in those areas where there is no difference in the rules between FAR Parts 27 and 29. In those areas where the rules are different, guidance for FAR Part 27 rotorcraft AFC applications is not contained herein. Such guidance is envisioned to be a product of the same evaluation methodology used to produce FAR Part 29 guidance herein.

(3) Applicability

The intent of this advisory guidance material is to ensure that AFC systems will have, at least, equivalent safety level characteristics as that provided by the existing rules when applied to conventional hydro-mechanical flight control systems.

A Functional Hazard Assessment (FHA) will use a rotorcraft’s operational functions to determine associated criticality categories and to identify the sources of failures that contribute to that determination, both in areas unique to AFC and in areas that are typical rotorcraft basic design. Both areas require evaluation, however, it may not be appropriate to evaluate those areas that are considered basic helicopter design using the guidance herein where existing guidance material is appropriate.

AFC systems generally consist of a control system that interfaces with some type of control actuator that in turn interfaces with some inherent control device providing

aerodynamic controls (swash plate and associated linkages are examples). Where the integrity of the basic design is adequately addressed by existing methods, they will not be addressed by this guidance. However, the FHA should include the complete aircraft flight control system. Basic rotorcraft design areas include, as a minimum, the existing controls that do not have to be different for a particular AFC configuration and structural aspects of the basic rotorcraft design. This does not preclude evaluation of these basic design aspects for AFC effects; it only means that the means of showing compliance for these basic design aspects are the same as for other considerations.

Applicability of the standards used in this guidance document is as follows:

RTCA D0160 / EUROCAE ED 14 (Environmental Conditions and Test Procedures for Airborne Equipment) -- New AFC equipment should use the RTCA document, D0160D, or later approved revision, if the later approved revision addresses the applicable environmental considerations to, at least, the same safety objectives that would apply for qualification to DO160D. Existing equipment, used for AFC applications that was qualified to revisions previous to DO160D, may be reused if the level of qualification is sufficient to address the safety goals established by the Safety Assessment (SA) process

RTCA DO178 / EUROCAE ED 12 (Software Considerations in Airborne Systems and Equipment Certification) -- Software for new AFC equipment should use the RTCA document, D0178B, or later approved revision, for a standard, if the later approved revision addresses the applicable safety goals established by the AFC SA to at least the same safety objectives that would apply for qualification to DO178B. Existing equipment, used for AFC applications that were qualified to revisions previous to DO178B (Reference FAA Order 8110.49, "Software Approval Guidelines"), may be used if the level of qualification is sufficient to address the safety goals established by the SA process.

ARP4761 (Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment) -- This document is accepted as a standard to define the SA process. Subsequent approved revisions may also be used as a standard to define this process.

ARP4754 (Certification Considerations for Highly-Integrated or Complex Aircraft Systems) -- This document is accepted as standard for the concept of the SA and system development assurance processes. Applicability of future revisions will be accomplished by evaluation for specific consideration at that time.

RTCA DO254 / EUROCAE ED 80 (Design Assurance Guidance for Airborne Electronic Hardware) -- This document is an accepted standard for device complex hardware that as a minimum includes PLDs and ASICs. Applicability of future revisions will be accomplished by evaluation for specific consideration at that time.

ADS-33E-PRF – Aeronautical Design Standard, Performance Specification, Handling Qualities Requirements for Military Rotorcraft, US Army Aviation and Missile Command, Aviation Engineering Directorate, Redstone Arsenal, Alabama, 21 March 2000.

b. Procedures.

This AFC Miscellaneous Guidance (MG) provides insight into some acceptable compliance methods for AFC systems that employ the previously described types of systems or other design variations. This guidance consists of several sections.

Section 1 is guidance on use of the Safety Assessment (SA) process for AFC. This section contains those pieces of AFC that can be addressed by the various sections of the safety assessment process and how to use the SA specifically for AFC systems.

Section 2 addresses the application of the safety assessment to specific rules and a methodology to show compliance to these rules when applied to AFC.

Section 3 addresses rules not specifically addressed by the Safety Assessment process. Guidance is provided on the intent of existing rules to assist in developing the content of special conditions that provide an equivalent level of safety.

Section 4 contains a summary table of rules that may require special conditions, and where available, referenced supporting advisory material. This table is a reference to guidance that addresses when a special condition may be required and how to recognize the need based upon present rules or issues that do not adequately address AFC.

SECTION 1

(1) Safety Assessment (SA) Guidelines for Advanced Flight Controls.

(i) Introduction.

The intent of this section's guidance is to define a way to show compliance to AFC requirements using the SA process, where applicable. The complex, highly integrated nature of AFC systems demands a thorough, systematic approach to evaluating malfunction effects. The SA process provides a framework for ensuring that possible failure paths are scrutinized to ensure that failure modes are adequately addressed.

The Safety Assessment (SA) process (ARP 4761) is a method that may be used to demonstrate certification compliance to applicable rules. The SA process consists of quantitative and qualitative parts that may be applied to AFC systems. An example of an area of the quantitative part of an AFC is failure/reliability analysis. An example of the qualitative parts of the AFC includes human factors, software, and pilot handling and reaction capabilities.

(ii) Definition of Terms

(A) Failure Condition – a rotorcraft or system level state resulting from a failure or combination of failures.

(B) Functional Failure

▶ Loss. The service provided by the function is absent.

▶ Malfunctions. A malfunction is defined to exist when the output(s) of the function do not respond properly to the associated input(s).

(C) Failure – the state of a system or component that results from a system or component fault.

(D) Fault – an undesired anomaly in an item or system that may cause a failure.

(E) Degraded operation -- Degraded operation of a function occurs when the output(s) deviate below nominal performance, but still provide at least minimal operational performance.

(F) Integrity –An attribute of a system or a component that can be relied upon to function as required by the criticality determined by the FHA.

(G) Complexity – Complexity, as addressed by this document, refers to integrated systems that exhibit characteristics that make deterministic effects of failures excessively difficult to comprehend without use of analytical tools. Additionally, complexity is used, in some cases; to address those integrated systems that may not be adequately evaluated by quantitative analysis alone.

(H) Latent failures - As used in this document refers to undetected failures that are not evident or active, either to the crew, for operational considerations, and/or to maintenance personnel, for maintenance considerations. The effects of latent failures may be mitigated, to some extent, by limiting the exposure time for latency of the failure.

(I) Error – An incorrect action or decision by personnel in specifying, designing, implementing, operating, or maintaining a system.

(J) Defect – A state of an item consisting of the non-performance of specified requirements by a characteristic of that item.

(K) Software Terms.

► Partitioning. This is the process of separating, usually with the express purpose of isolating one or more attributes of software, to prevent specific interactions and cross-coupling interference.

► Protection. This is a concept, which ensures the separation of systems functions, so that a fault in one function cannot affect another. Protection is typically considered a superset of partitioning.

(L) Other Terms

Inceptor – This term is used herein to describe the pilot’s control implementation device, which may also be called a “controller”, “side stick”, “collective controller”, etc.

(iii) Application of the Safety Assessment Process

The safety assessment process consists of three parts: Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), and System Safety Assessment (SSA). A safety assessment process and the need for it are generic in nature, as it is only a structured compliance method and not the only compliance method. From a generic position, explanation of the application of the safety assessment is provided by SAE document ARP 4754 and the SA process itself is defined by SAE document ARP 4761. Generic information about the use of the SA process for showing compliance to §§ 27.1309 and 29.1309 is provided from the MGs of their respective AC 27-1B, Change 1, and AC 29-2C, Change 1. Guidance will be provided to show how to apply the SA process to specific issues/functions of AFC systems herein.

The three most important aspects of AFC systems as they relate to the SA process are functionality, potential failures, and considerations for the complex integrated designs.

The SA process should address AFC functionality from a preliminary design aspect and from the developed AFC system. This will be provided by a part of the Functional Hazard Assessment (FHA) accompanied by certain basic assumptions, and the Systems Safety Assessment (SSA), respectively. These assumptions are adequacy of functionality associated with flight operations, control laws, and failure management. The safety assessment process should provide the necessary assurance that all relevant failure conditions have been identified and that all significant combination of failures that could cause those failure conditions have been addressed.

It is generally not practical, or possible, to develop a finite set of tests to prove that the system complies with system safety objectives. Therefore, other means of showing compliance is needed. The SA process, in conjunction with development assurance processes as described in ARP-4754, establishes a means to ensure that the AFC system has been developed in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety beyond acceptable levels.

(A) Preliminary Steps for System Safety Assessment (FHA/PSSA)

The combination of the FHA and the PSSA is a methodology to define the safety objectives related to system functions and therefore derive safety requirements for the design.

The first step of the preliminary system development process is the Functional Hazard Assessment (FHA). Starting from the AFC functional specification and flight operations, failure conditions associated with the AFC functions are identified and classified.

As a second step, a preliminary Fault Tree Analysis (FTA) of the PSSA is conducted. The proposed system architecture is examined to identify the equipment involved in generating the functional failures defined by the FHA and the expected failure probabilities are estimated. By comparing these against the probability objectives related to the failure condition categories, it can be determined that the proposed architecture can be expected to meet the safety requirements.

The third step is conducting a preliminary Common Cause Analysis (CCA), which includes three types of analyses: a) Zonal Safety Analysis (ZSA), b) Particular Risk Analysis (PRA), and c) Common Mode Analysis (CMA). With the ZSA, the design is checked for appropriate equipment installation and potential interference with/from other systems. With the PRA, the effects of external threats such as fire, lightning strikes, or High Intensity Radiated Fields (HIRF) upon the system are analyzed. The CMA looks for single events, which may cause multiple faults or loss of function from an availability or malfunction standpoint. As for the preliminary FTA, the proposed system architecture is checked by the CCA to determine that the system can be expected to meet the safety requirements and that the FTA events are truly independent.

(B) System Safety Assessment (SSA)

The SSA is a set of evaluations/tests that show the safety requirements and design goals established by the FHA and other analysis have been met. The methods of showing compliance for AFC are unique in some cases. This is particularly true for the allocation of functionality to parts of complex integrated systems, possibly software driven. The methodology used to perform these evaluations includes failure considerations, pilot vehicle interface, hardware/software/systems assurance, failure management, and validation of common cause analysis and verification that all safety requirements are addressed. Guidance for the evaluation methodology is provided for AFC items as follows:

The SSA consists of various bottom-up analyses and validation of the preliminary CCA. Failure probability figures used for establishing the preliminary FTA is derived from a detailed bottom-up failure analysis for the equipment. The data obtained from this bottom-up analysis is utilized to validate the preliminary FTA or to modify the FTA to accomplish the top down safety considerations.

(C) Ingredients of the PSSA/FHA and SSA Processes

The ingredients of the PSSA/FHA preliminary design activities and the SSA mature design evaluation activities are the SA process. The ingredients as addressed by this document section are an accumulation of activities that fit into one or more parts of this SA process of development.

(1) Functional Hazard Assessment (FHA).

The aircraft level FHA is the first step in the SA process. The result of aircraft level FHA is the input to the aircraft level PSSA, including associated aircraft fault trees, and is the input to the system level FHA. This process defines the criticality of the assessed functions that are used to determine the required integrity level for the system components.

A system may be evaluated by an FHA as a top-down process as described in the Advisory Circular (AC) of the related FAR 1309 (FAR 27 or FAR 29) or ARP 4761, paragraph 3.2. The assumptions that form the baseline for each FHA must be defined as a starting point for the FHA. As an example, some of the assumptions for the aircraft FHA are based on flight limitations/operations and the previously addressed "Validation of Pilot-Vehicle Interface Assumptions."

This portion of the SA that is a top-down approach will provide a basis for determination of the related failure condition categories for the considered failures. Failure condition category definitions are defined in AC 27/29 for FAR part 1309. The FHA is an analysis of a system's functional breakdown to a level that can be used to determine hazards, including consideration for failures of non-AFC related functions. These evaluations may be done at the AFC system level or aircraft functional/operational level.

(i) AFC Failure Condition Considerations

There is a need to consider all types of AFC functional failure conditions to account for the resultant predicted flight control behavior in the FHA.

The determination of failure types can be obtained from the functional allocation. If necessary, according to the context, the type of the failure (detected and/or non-detected) is stated precisely in the failure identification. The different types of failure conditions have different degrees of impact on AFCs and therefore represent different failure condition categories. These include loss of function, malfunctions, and degraded operation.

Examples of sources causing potential AFC malfunctions for design consideration are:

Limit Cycles: Limit cycles are typically caused by non-linearities combined with high control gains and should be minimized and reduced to an acceptable level. Typical non-linearities in flight control systems are poor resolution of digital signals, control signal limitation (e.g., actuator rate saturation), and hysteresis (e.g., backlash of

bearings). Limit cycles may affect controllability and make the system prone to Pilot Induced Oscillations (PIO).

Spurious Data: Spurious data can be caused by signal perturbation from external sources (e.g., sensor noise, electromagnetic interference) or defects of equipment (e.g., loose electrical contact). The effects of spurious data upon the performance of the flight control system ranges from minor to catastrophic, depending on the interference severity.

Aliasing Effects: Aliasing effects are caused by analog-to-digital conversion of sensor signals, which contain significant signal noise at frequencies above the sample frequency. The high frequency noise is converted into a low frequency signal, which is superimposed to the original sensor signal. The effect is a distortion (e.g., D. C. offset) of the measured signal.

Oscillatory Failures: Oscillatory failures can be caused by a number of effects: system instability due to a corrupted sensor signal (e.g., angular rate), oscillatory excitation from a corrupted hardware component (e.g., operational amplifier), or excitation of resonance frequencies (e.g., air resonance, structural resonance of tail rotor shaft).

Runaways/Hardovers: Signal runaways or hardovers can be caused by a generic hardware and/or software design errors. Additionally, they may be caused by failures within the flight control computer or a sensor or by a jammed servo valve in one of the actuators.

Jams: Jams address movable mechanical parts of the flight control system (pilot's controls, actuators) that experience limitation of required movement, for example, by foreign objects, corroded bearings, or icing.

False Alarms: False alarms (warnings, cautions) can be triggered by monitors, which are too sensitive because the monitor thresholds and/or failure confirmation times are too small.

(ii) Failure condition classification.

All AFC failure conditions must be classified. This classification is based on the identified effects described in the AC 29-2C 1309(f), i.e., Catastrophic, Hazardous/Severe-Major, Major, Minor, and No Effect. The circumstances of the failure occurrence may have strong impact on the failure severity and therefore, the classification of every failure condition should be determined taking into account the full range of rotorcraft operation. Failure condition effect(s) can be different according to the flight phase: near the ground or in cruise or in approach or over the sea. The entire flight envelope must be evaluated when determining the failure condition classification. All the operational phases must be taken into account including the ground phases (the rotor must remain controllable during hydraulic shutdown for instance).

It is necessary to identify the environmental conditions that can affect the classification of AFC failure effects. For example, the level of atmospheric disturbance shall be considered when defining the classification of a failure condition. Furthermore, the piloting conditions such as Visual or Instrument Meteorological Conditions (IMC) must be addressed since failure effects can vary significantly.

Evaluation of the severity of a failure condition must address the transient effects following the failure occurrence as well as the resultant handling qualities. Certain assumptions about pilot actions, skills, strength and ability, and aircraft response relating to AFC failures will have to be made to determine the failure mode classification. AFC failures may occur in either automatic or pilot initiated reversion to modes of operation that are intended to allow continued safe flight but with a reduced level of Handling Qualities (HQs), or reduced levels of safety. To show compliance with the safety requirements contained in Part 29, Subpart B, the underlying assumptions and analytic techniques should be identified and justified to assure that the conclusions of the FHA are valid. Justification of the assumptions should be an integral part of the analysis. Assumptions can be validated by using experience with identical or similar systems with allowance made for differences in design or operating environment. Where it is not possible to fully justify the validity of the assumptions, or where high variability is expected, and the assumptions are critical to the acceptability of the failure condition, then extra conservatism should be built into either the FHA or the design. The SSA on the developed system should validate these premises.

Examples of assumptions to be made should, as a minimum, include:

- The pilot's ability to correctly identify the nature of failures and identify the correct procedures.
- The pilot's ability to correctly accomplish Flight Manual procedures to reconfigure controls, in response to AFC failures.
- The intervention time is adequate for the pilot to deal with the failure condition and any associated aircraft response.
- The pilot's ability to control the rotorcraft with degraded handling qualities for a period of time appropriate to the intended use of the rotorcraft and for the full range of operating conditions covered by Part 29, Subpart B regulations.

(2) Fault Tree Analysis (FTA).

The FTA is initially performed by assigning design assurance budgets to the AFC inputs, that drive the top events, identified as having a high criticality by the combination of aircraft level FHA and system FHA. When actual AFC design data is available from the design evaluation performed in the SSA, the SA FTA is finalized and a comparison evaluation is made to the preliminary FTA, which determines if design goals have been

met. This analysis will show how the lower level failures can lead to the functional hazards identified by the top level aircraft FHA and the AFC FHA and how the defined failure condition categories driven requirements will be met. This analysis must take into account the preliminary Common Cause Analysis to identify where robustness must be put on the system.

When performing bottom-up failure analyses to prove that the PSSA goals are met, the basic assumptions made when the safety goals were established should be validated. Examples of these basic assumptions include IMC, HIRF, or crosswind operations under which the rotorcraft is approved to operate. On the other hand, reasonable and rational consideration of the statistically derived probability of an emergency condition may be included in the safety assessment, provided it is based on applicable supporting data. An example of the reasonable and rational considerations is the aspects of an engine failure followed by loss of a collective lever tactile cueing system that helps the pilot maintain rotor speed in a One-Engine-Inoperative (OEI) condition. However, the probability of an engine failure should not be used to lower the integrity of AFC functions that can have catastrophic failure effects regardless of the engine failure state.

When considering the derived probability of such an emergency condition with that of an AFC failure, care should be taken to ensure that the condition and the AFC failure are independent of one another, or that any dependencies are properly accounted for, in the FTA. For example, the combination of engine failure and AFC faults that result from a common cause must be considered (e.g., uncontained engine failure) and is typically treated as a single fault. Another example of multiple failures caused by a single fault is an engine failure combined with loss of electrical power from an engine-driven generator.

The PSSA FTA inputs are generally generated from undeveloped events, which should take in account the possible failures coming from the AFC components (equipment, rods, wiring, etc.) and in conjunction with other systems (Hydraulic, Electrical, Cooling, Weight on Wheel, etc.), common cause failures, dormant failures, etc.

The following are examples of the top-level failure event addressed by the system level PSSA FTA:

- loss/malfunction of the four axes control
- loss/malfunction of one axis control
- loss/malfunction of one actuator control
- loss/malfunction of the control and stability augmentation system on the four axes
- loss/malfunction of the control and stability augmentation system on one axis
- loss/malfunction of mode annunciation

(3) Preliminary Common Cause Analysis (CCA).

(i) Introduction.

The preliminary CCA, a part of the PSSA, identifies common causes for faults/malfunctions. The potential for failures/malfunctions due to common cause is inherent in designs that provide multi functions reliant on common hardware or common software. This is also true for systems that provide related functions and share a common installation area. Apart from design deficiencies, manufacturing or maintenance errors could also impair AFC system component independence. In addition, the installation area may represent a threat from several sources such as Electro-Magnetic Interference (EMI), mechanical hazards, and environmental influences.

To provide a structured approach to perform common cause analysis, the analysis can be divided into subparts as follows:

(ii) Zonal Safety Analysis (ZSA)

The ZSA examines the physical zone of the rotorcraft, in which the system under consideration is installed, to insure that the surrounding equipment/appliance installations do not compromise the AFC system independence requirements. Overheat fluid leakage and vibrations are examples of the type of event that would be considered for an AFC ZSA.

Another important aspect is proper separation for the reasons as follows:

- To address the effects of failures in relation to other systems/equipment
- To address the implications of maintenance errors.
- To address the FTA assumptions for the design.
- To address the basic standards of design and installation.

(iii) Particular Risk Assessment (PRA).

The PRA considers similar risks to the ZSA except that it considers those risks that have an origination source outside the system and possibly for events that affect more than one rotorcraft zone. HIRF and lightning are types of particular risks that should be considered, particularly for AFC redundant applications. PRA also considers mechanical failures that might generate fragments that could damage the system under evaluation, such as engine non-containment or bird strike.

(iv) Common Mode Analysis (CMA).

The CMA is the part of CCA that is the most intensive for the AFC system design under evaluation. The CMA considers many aspects of the AFC system design; one is design diversity (dissimilarity) for both hardware and software. Without diversity (dissimilarity) for redundant design elements, there is a possibility that a hardware or software failure/malfunction could occur in the same flight for all redundant subparts of an AFC system invoking an unacceptable level of risk. Another major contribution from the CMA is the determination of which failure/malfunction combinations of inputs to the

Fault Tree Analysis (FTA) must be independent for events that are catastrophic or hazardous-severe. This analysis is iterative in nature, as it will be employed early in design to identify possible causes for failures/malfunctions and then is used after the design is complete to determine if the FTA goals have been met.

(4) Validation of CCA.

(i) Introduction.

Validation of the CCA, part of the SSA, provides the comparison data to assure the preliminary goals are met. Following detailed analysis of common cause for fault/malfunctions of the AFC systems, the validation process should:

Address proper resolution of common modes.

Show adequate methods to substantiate environmental assumptions.

Include an extensive zonal analysis, to determine that all common threats to the systems have been properly addressed by design and installation needs.

(ii) Common mode validation.

As previously stated in the CMA definition, design, manufacturing, and maintenance of the AFC should be evaluated to ensure that the required independence is protected from errors or defects.

(iii) Dissimilarity.

There are several means to protect a system that provides critical functions from common mode failures of redundant elements. For example, when the AFC architecture incorporates redundant elements of similar components, the components can be developed to a high level of assurance to protect against generic design faults. During the manufacturing process, adequate quality controls may be implemented to protect against common manufacturing defects. Methodology to provide this means of compliance may mean extensive qualification testing, manufacturing burn-in and component screening.

Alternatively, when system architectures consist of redundant subsystems for critical functions, dissimilarity maybe a method to preclude a common mode failure specifically for complex components that contain failure mechanisms that cannot be readily determined. Dissimilarity is one method to address the possibility of common mode failures for hardware items, such as microprocessors, since these devices are typically very complex and it is impractical to test all operational aspects completely. Other complex hardware components (e.g., ASICs, PLDs) that have a high level of risk associated with their intended function may be candidates for dissimilarity between redundant implementations, for the same reasons. When dissimilarity is implemented in software, it may be introduced at one or several of the following points during development:

- Dissimilarity of Functional Requirements with software implementation
- Software structure that may compensate for hardware similarity
- Generation of different binary object code using different compilers/assemblers

In these cases, functional failure occurrence will be largely affected by the level of dissimilarity employed.

(iv) Methods to validate environmental assumptions.

Environmental assumptions which are allocated to the affected parts of an AFC system need to be validated by showing proper operation of these parts through the dedicated parameter range. The methodology to provide this validation usually includes one or more of the following: extensive analysis, laboratory testing, ground tests, and flight tests. When the environmental assumptions are, at least in part, dependant on zonal requirements, the compliance to these requirements should be evaluated using the environmental assumptions as criteria.

(5) Preliminary Reliability Analysis.

When failure rates are assigned as goals in the PSSA/FTA to meet an AFC function's related failure condition category, it may be necessary to verify that the assigned values are reasonably possible. The feasibility of the assigned failure rates to new AFC equipment designs is determined, for the most part, by a preliminary reliability analysis. The same process is used for any reliability analysis, but the preliminary reliability analysis is typically performed using a non-verified design baseline, whereas a full reliability analysis is performed using failure rates of actual components. Because the equipment's final design is not known at this point in the development process, the preliminary reliability analysis is based upon manufacturer component specifications. This information is not only preliminary in design implementation (circuit design, parts count, etc.), but in operating characteristics as well. Some of the assumptions for the preliminary reliability analysis involve temperature, operational exposure time, integration considerations, and other environmental concerns.

(6) Bottom-up Analysis.

Many types of bottom-up analysis are employed to evaluate and provide data for comparison to the design goals assigned by the preliminary FTA.

Examples of bottom-up analysis include:

- Reliability Analysis
- Failure Modes and Effects Analysis

One bottom-up method of identifying failure modes of a system, component, or function and determining the effects on the next higher level is a Failure Modes and Effects

Analysis (FMEA). There are other names for this type of analysis that may provide the same information, and possibly additional information that is addressed herein. Where FMEA is named herein, these other types of analysis may also be valid to use for acquisition of the addressed data.

Typically, an FMEA is used to address effects resulting from single failures. These types of single failures, for the most part, are those resulting from faults that are independent and cannot cause a catastrophic event by themselves. No single AFC fault and resulting failure is allowed to cause a catastrophic event. Quantitative consideration for a single fault/failure is not applicable to inherently single string flight control path components, typically mechanical, hydro-mechanical, and electromechanical devices. Some faults and their resulting failures have no realistic database for probability of occurrence, due to the high degree of variance associated with them. Failures that do not have a known realistic database must have compensation provided by design to provide fault tolerance to facilitate AFC systems compliance for the associated safety goals. For failures that do have a realistic database, the failure rates can be calculated. Before a calculation of the failure rate can be attempted, the failure should be defined. The determination of failure rate, using the definition of failure, can be the product of an analysis combined with a reliability analysis, using individual part reliability figures. Reliability figures should come from some recognized database. Failure rate calculations should consider the worst-case application limitations, such as flight operations, environmental considerations, and time of operation. The calculation of failure rate is a direct result of the FMEA and that data should be used for comparison to the PSSA FTA values.

FMEAs, or equivalent analysis, typically include the following:

- Identification of component, signal, and/or function
- Failure modes and associated hardware failure rates
- Failure effects
- Means for fault detection

Additional parts of the FMEA may include considerations to identify single or multiple failure effects that will affect integrity requirements. Both qualitative and quantitative analysis can be useful to accomplish these identifications.

(Z) Development Design Assurance for Systems and associated Hardware/Software.

In the initial development process, design assurance levels should be determined for all aspects of AFC systems design, including the preliminary phases addressed by the PSSA/FHA and the mature design phases addressed by the SSA, as defined in RTCA 4761. Design assurance activities must cover validation of the requirements for the function and verification of the correctness of the functional design to meet the requirements. Additionally, these activities should assure that the specified functional design is correctly implemented in hardware and/or software. These activities assure

that the design meets the specified performance, reliability, and availability for all intended operating conditions. There is no difference in this methodology from any other type of system except from a functionality and criticality aspect. These aspects are discussed in the following paragraphs.

(i) Systems Development Design Assurance

The primary goal of any design is to provide the specified functionality without unintended effects. AFC systems have the same goal, but have some unique aspects. AFC systems development design assurance starts with the systems requirements capture, during validation of the design requirements. Typically, system design depends heavily upon complete and correct system requirements, which include elements of performance to meet the mission, functionality needed to execute the mission, safety/reliability, man-machine interfaces to assure good handling qualities, and operability, maintenance, and dispatch, design cost, etc.

These requirements are then allocated to subsystems, arranged in a system architecture of elements arranged in series/parallel signal processing paths to perform the functions and meet their ancillary requirements. The great majority of in-service system problems are traceable to inadequacies in the system requirement specifications and in the validation of the correct functional design for all its intended operating conditions. System requirements are the starting point of the AFC design and these requirements should be substantiated during the preliminary design/evaluation activities phase of the system development program. The preliminary system functional designs are used as the basis for the FHA and for the system architectural design, which forms the basis for the PSSA and later for the SSA.

Completeness and correctness of the functional design must be verified systematically, first by the PSSA and later by the SSA activities when AFC design matures to a level that allows evaluation and tests on actual system components. This is one of the most difficult system analyses processes, because it requires a very detailed understanding of all system elements and their possible interactions, during both normal functionality and failure/fault functionality conditions, including combinations of modes and operating conditions. This may involve exhaustive computer analyses, laboratory testing, and possibly flight-testing, to validate that system requirements are correct and the functions are designed correctly. Computer analyses may need to include system state analyses to systematically probe for conditions that may result in invalid system or mode control logic states, as well as simulations to check design robustness. Modern AFC designs tend to tightly integrate many functions (modes) and in-line and parallel system components, resulting in numerous possible system states. Invalid system or mode logic states often result in failure of the system to perform its intended function, or in an unintended function. The functional design assurance process must identify and eliminate both, preferably at the earliest possible stage in the system development. This often involves iterations of the design requirement specification and the functional design. Validated system requirements and function design is the key to correct system hardware and software requirements specification and implementation.

Some of the considerations to be used or analyzed in the validation process for the AFC design are as follows:

- Control law evaluation
- Simulation (e.g. computer, flight, etc.)
- Modeling (e.g. wind tunnel, control surfaces, etc.)

Some of the considerations for evaluation of systems that comprise AFCs are as follows:

- Sneak circuit analyses
- Timing
- Tolerances
- Persistence

Some methods to validate the AFC system design specifications and the related AFC system design assurance goals after the design is adequately mature are as follows:

Computer analysis/simulation to validate the control laws (stability, bandwidth, phase delay, step response, and parameter sensitivity).

Bench tests to validate equipment performance (e.g. mode and failure logic, computer through put, and actuator dynamics).

Rig tests to validate system performance (e.g. response characteristics, switching transients, and reaction to failures).

Flight simulator tests to validate handling qualities (controllability, and failure effects).

Ground tests to verify system integrity.

Flight trials to verify that the system performs as specified and as predicted by analysis, and simulation.

Analysis for hardware and software verification activities (e.g., traceability, reliability, structural coverage) and tests (e.g., endurance, robust, seeded failure/fault), to show that the system design assurance goals set in the PSSA/FHA are met by the actual design that is installed in the rotorcraft or installed in a simulated installation.

AFC systems are typically part of complex integrated systems that provide more than one category of functionality. Guidance for complex systems integration is provided by ARP-4754 and MG 13 of AC 29-2C, Change 1. Evaluations of AFC systems that are a part of complex integrated systems have unique concerns, in addition to the AFC unique concerns, that are independent of integration issues of other systems. The same processes may be used to perform these evaluations, but additional

considerations should be addressed. The major thought process applied to these considerations is:

- System availability
- Misleading Indication and/or Crew Interfaces
- Excessive Flight Control induced loads.

One of the main considerations for AFC design is that the design requirements for availability do not result in excessive complexity. This could defeat the availability effort by increasing the number of opportunities for failures, including common failure mode possibilities, and greatly increase the concern for design errors, as well as complicate design evaluation. In very complex circuits, it may not be possible to totally test all functional possibilities. Design errors may be mitigated by redundancy/failure management and by parts of the SA. However, the result of systems that employ mitigating features in their design is a trade-off between Built-In Tests (BIT)/failure management systems and design goals for lower complexity. Another consideration for AFC design is common cause failures that could result in defeating the intent of redundancy. Many of the detailed methods to address these concerns are contained in the following paragraphs for hardware and software design assurance.

(ii) Hardware Development Design Assurance.

RTCA document DO254 addresses the design life cycle processes necessary to provide hardware design assurance in accordance with the integrity goals set by the PSSA. This RTCA document provides a mapping of processes and design goals for development of PLDs and ASICs complex hardware, as well as classic LRUs, and their major subassemblies. Although it is recognized that other aspects of hardware design assurance exist the focus of hardware design assurance for AFC systems hardware in this guidance document is directed to considerations for functionality, a determination of reliability, and environmental considerations. Elements of hardware design assurance are in the PSSA and the SSA.

(a) Development Design Assurance for Functionality, Allocated to Hardware.

AFC hardware design assurance is related to the AFC system requirements primarily by allocation of functions. The functions allocated to hardware should be implemented to provide specified performance within the required availability/malfunction allowance and in the assigned environment. These constraints must be true for a normal AFC operational state and for one or more managed failure operational states. These managed failure operational states are defined by the design goals established by the PSSA/FHA process and verified by the SSA. Since AFC systems typically provide flight operational functions that have high criticality categories associated with them, the AFC systems usually consist of multiple layers of redundancy/back-up. The hardware for these systems must provide the specified performance and the redundancy management/failure detection that are relegated to the hardware portions of the AFC.

Additionally, AFC design must address common cause failure possibilities, particularly for hardware, to preclude negation of the positive effects of redundancy. One method to address this failure mode is dissimilarity(see paragraph on dissimilarity above).

(b) Hardware Reliability.

The most accurate measurement of reliability is service history. However, new designs seldom can benefit from service history, because by definition, the design is new and has little or no history of any kind. Additionally, when service history is used, it should be relevant to the hardware item being evaluated for the aircraft platform, application, and environment. Another possibility for the determination of reliability is testing over a relatively short period of time using more severe conditions equivalent to a longer period of usage. The most common method used to make a determination of reliability is analysis. This type of analysis is bottom-up and is performed as a part of the PSSA for preliminary design predictions, and as a part of the SSA, after design is at sufficient maturity. If this method is used, a relevant database should be used. Examples of frequently used databases are MIL STD 217, Non-electronic Parts Reliability Data (NPRD-95), or Failure Mode/Mechanism Distributions (FMD-97) from the Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916. New AFC designs may employ some parts that have been used in other applications, and as such, these parts may be candidates to have a relevant history for reliability determination. The deciding factors for service history relevancy are typically similarity of design and similarity of application. Similarity of design is partly subjective and is difficult to address from a generic approach. An example might be a hydroelectric actuator. The actuator to be qualified by similarity should have very similar functional capability, and have the same or better environmental qualification and be essentially constructed from the same materials using the same processes as the actuator from which service history is claimed. Only favorable service history can be claimed and fixed problems do not make it possible to reclaim previous unfavorable service history as favorable after the fix. The use of a similar part presumes that the application is also similar. For this example, similarity of application should consider actuator loading, required speed, environment, and physical attachment as a starting point. AFC relevant service history is difficult to find, due to the vast differences of applications such as operations, environmental exposures, and maintenance procedures. Where it is not possible to fully justify the reliability predictions, extra conservatism should be built into either the analysis or the design. Any uncertainty in the data and assumptions should be evaluated to the degree necessary to demonstrate that the analysis conclusions remain valid.

(c) Hardware Environmental Considerations.

Hardware components should be designed to be compatible with the environment in which they must function, and be available within some reasonable expectation. The degree of reasonable expectation is associated with the particular function or group of function criticality. An acceptable standard for qualification to environmental considerations is RTCA Document DO 160. New equipment should use the latest revision. However, there may be some circumstances that use of an earlier revision

may be appropriate as long as the actual environmental conditions of the equipment installation are adequately addressed. AFC systems will be for the most part new systems. Generally, this standard supplies a qualification method for the various environmental conditions, but must be supplemented by the actual data of the intended installation. An example would be a rotorcraft that had unusual vibration characteristics and the installed equipment would have to be qualified to a higher level of vibration than that provided for rotorcrafts in DO 160. Environmental qualification of equipment that has been assessed to be either Catastrophic or Severe Major/Hazardous should focus not only on the possible loss of function, but also on the misleading or malfunction aspects. This additional level of concern is for the most part addressing electromagnetic interference, from either High Energy Radiated Fields or lightning, but not limited to these two sources. Environmental qualification by similarity should be limited to actual similarity to the product, not similarity in incremental steps. This addresses the example of several changes to a product over time, each of which was minor, and resulted in a similar product to the preceding one, but the end configuration was not similar to the initial product. Environmental qualification for AFC components is challenging as the components are widely dispersed over the rotorcraft and encounter a number of different physical environments. Preliminary design considerations for environment are addressed by the preliminary CCA of the PSSA, and the mature design provides data for the CCA validation in the SSA.

(iii) Software Development Assurance.

Software development assurance is provided by using RTCA DO178B/ED12. As a software development standard, it is one possible method to show compliance to the rules that mainly addresses quality. The criticality category determined for the AFC functions will set the assurance level for the software. The availability, and to some extent, the misleading aspects for software considerations, are not necessarily unique to AFC, except for the uniqueness associated with the functionality and the typical layering of redundancy. However, the flight control induced loads aspect is unique to flight controls and AFC, in particular, because of the possible failure modes. Common cause failures that can result from the application of the same software between redundant implementations should be considered. In some cases, common cause failures are addressed by dissimilar software. Research results (reference International Electrical, and Electronic Engineering paper, titled Analysis of Faults in an N-Version Software Experiment, Vol. 16, No. 2, dated February 1990, written by Susan S. Brilliant, John Knight, and Nancy G. Levenson) have shown that dissimilarity is most effective when employed as a combination of software and hardware architecture. Dissimilarity in software coding alone has yet to be shown to be effective to preclude common errors, between redundancy implementations. Other considerations to address common cause software errors in redundant AFC elements are Level A development assurance or software partitioning. Partitioning (i.e., safety protection) can be used to isolate the effects of faults between non-related functions with different levels of criticality.

AFC systems may combine many functions of different software levels on the same AFC target computer. Per RTCA/DO-178B, higher level(s) software must be partitioned

and/or protected in such a way that lower level(s) software cannot affect the memory locations allocated to the higher level software or otherwise interfere with the computation of its functions (that is, there must be both time and space protection). It should be noted that functions operating on the same hardware might need to be partitioned and/or protected to support fail-safe designs and safety requirements, even if they are the same software level (i.e., functional partitioning). Functional partitioning is recommended as a means to reduce complexity and provide adequate fault containment. Typical design features that implement partitioning should use both hardware and software means.

(8) Failure Management.

Failure management is important to AFC systems since the ultimate worst-case effect can be catastrophic. Failure management is a set of design features that are in part specified and are in part derived requirements. The FHA will identify the possible failures that are in need of management to preclude the loss of rotorcraft or that could lead to the loss of rotorcraft. Once failures that need management are identified, the necessary design attributes are addressed by the FTA and later evaluated by the SSA activities.

Some types of failure are:

- ▶ Functional failures due to hardware or software design errors (generic faults).
- ▶ Functional failures due to hardware failures caused by material aging, fatigue, stress, corrosion, jams, or excessive environmental conditions (e.g., temperature, vibration), or random failures.
- ▶ Functional failures due to excessive external disturbances (e.g., electromagnetic interference, lightning strike).
- ▶ Functional failures due to parts substitution or manufacturing problems.

Failure management is required throughout the whole life cycle of the flight control system, including the development phase, the production phase, and the operational phase of the rotorcraft.

Failure management methods include the following elements:

- ▶ Tests with external test equipment, and in case of failure, equipment redesign and/or repair
- ▶ Initiated tests with built-in test functions and replacement of faulty equipment by spare units

▶ Redundant system design with continuous in-flight monitoring and system re-configuration in case of failure

▶ Fault tolerant design that prevents equipment faults from creating a functional failure

(i) Failure Management during development.

Failure management during development includes a variety of equipment and system verification tests to identify and eliminate design errors:

-Qualification tests with special test equipment to demonstrate that the equipment design meets performance requirements with respect to control functions and safety functions within the specified range of operational and environmental conditions

-System tests on a test bench/rig under normal operating conditions and simulated failure conditions to demonstrate correct operation of the integrated system-

-Ground tests on the rotorcraft under normal operating conditions and simulated failure conditions to demonstrate correct operation of the integrated system when installed in the aircraft with real aircraft wiring, power supply, and cooling

In case of failure a redesign of the affected equipment/sub-system may be required.

(ii) Failure Management during Production

Failure management during production includes equipment and system tests to identify and eliminate manufacturing problems:

-Burn-in tests, i.e. temperature and vibration cycles, to stress each individual unit of equipment prior to delivery to eliminate units with material defects and/or poor manufacturing. For AFC systems, burn-in tests are considered necessary to show compliance for continued airworthiness requirements.

-Acceptance tests to check correct functioning of each individual unit of equipment prior to installation

-Ground tests on the rotorcraft to demonstrate correct operation of the integrated system when installed in the aircraft

In case of failure, the affected equipment has to be recycled for repair.

(iii) Failure Management during Rotorcraft Operation

(A) Ground Testing

To keep the flight control system in a healthy and safe operational condition and maintain continued airworthiness during operation of the rotorcraft, system tests have to be performed on a regular basis or, respectively, on-condition. Some examples are:

- Pre-flight tests to check system availability prior to take-off

- On-condition maintenance inspection and tests to localize faulty equipment after a functional failure has occurred in flight and to verify correct operation of the system after replacement of individual units of equipment

- Scheduled maintenance tests to limit the effects of failures from equipment with the potential for latent faults. An example would be to have scheduled tests for redundant control paths to limit the exposure time for a latent failure that could result in total loss of control.

- Acceptance tests after repair and prior to re-installation of equipment

- Re-qualification tests of equipment after original parts have been substituted

(B) Built-in Failure Management

Although during development and production the equipment is thoroughly tested to eliminate faults, and during operation efficient maintenance procedures are applied, the occurrence of failures during flight is inevitable. For this reason, flight control systems must be fault tolerant, as a complete loss of the flight control system due to a failure should be extremely improbable.

The two principal methods to achieve fault tolerance are:

- Continuous monitoring with redundancy management

- Robust design.

(1) Continuous Monitoring and Redundancy Management

Continuous monitoring and redundancy management, for detected failures, provides isolation for the faulty part of the system, and provides, from the remaining part, the necessary functions, or alternate control.

Failure detection and redundancy management, in principle, is not much different for AFC, than for other systems, except for the functionality aspects. The typical degree of redundancy for AFC dictates complex, sophisticated redundancy management systems. AFC systems typically employ high levels of redundancy to address availability/reliability. This high level of redundancy makes redundancy management

complex. In the end, redundancy management consists of the usual failure detection mechanisms with the coupled resultant actions. These actions may consist of an annunciation to the crew with or without manual or automatic reversion to some layer of redundancy. The hierarchy of reversion to layers of redundancy is more important for AFC systems than for other systems as the number and consequences of possible effects is greater. The redundancy management often contains as many functions or more functions than the primary part of the AFC.

Considerations for AFC redundancy management are given as follows:

One or more of the following means may accomplish fault tolerance by redundancy management:

- With a redundant (i.e., multiple channel) AFC system, all control channels are operating in parallel and their output signals are consolidated. In case of a detected failure, the affected control channel is deactivated or isolated, and the remaining channels provide the required functionality.

- Faults that cannot be continuously detected by the monitoring system must have a probability of occurrence consistent with their failure classifications. The period of latency is used to derive the probability of failure occurrence.

- Alternatively, with a redundant AFC system, one channel is active while the other channels are on standby. In case of a detected failure, the affected control channel is deactivated and replaced by one of the standby channels, which then provides the required functionality.

- With a redundant AFC system, which is composed of a (redundant) primary control system and a dissimilar back up, the primary system is normally in operation while the back up is on standby. In case of a total failure of the primary system, the back-up system takes control.

- Continuous monitoring is performed individually within each control channel by a number of features, such as voltage comparators, input data monitoring (validity, parity, update, range), memory checks, and watchdog timer, to detect potential equipment failures and system malfunction, such as signal runaways and oscillatory failures. Sufficient computer throughput to accommodate this function must be provided.

- Dissimilar hardware and software, combined with cross monitoring between dissimilar channels, may be used to detect potential generic faults.

- Failure logic is used to confirm failures, trigger redundancy management, possibly re-configure the system, and generate failure warnings or cautions.

-Warning and caution indications are displayed in the cockpit to alert the crew and inform the pilot about the state of system degradation/failures. Information is displayed to tell the pilot which actions have to be taken, e.g., to fly hands-on and/or to stay within a reduced flight envelope.

-Bus/System architecture design considerations for redundancy management implementation

Examples of failure effects on elements of the AFC used for redundancy management are as follows:

-After partial failure of the AFC system redundancy, the reliability of the system is reduced.

-A corrupted monitor may either not be able to detect system failures or detect non-existing failures. The first case may lead to a hazardous situation since the system is not able to react appropriately to failures (i.e., system re-configuration, warning indication). The latter case may have a significant effect on the system by unnecessarily causing the redundancy management subsystem to degrade the AFC system from either a control aspect or integrity aspect.

-A faulty warning or caution indication may either not be able to indicate existing failures or indicate non-existing failures. The first case may lead to a hazardous situation since the system is not able to alert the crew after the occurrence of failures. The latter case leads to false alarms, which may overload/distract the pilot, if it happens too frequently. Hence, excessive false alarm rates have to be considered a safety problem equivalent to the inability of a monitor to detect failures.

Methods to achieve and maintain the safety functions of the elements used for redundancy management, for example are:

-Built-in tests, including power-up tests, for pre-flight checks should be provided to check availability of the equipment and correct operation of the monitors and warnings before take-off.

-Monitor thresholds should be set to values which are neither too wide, to avoid excessive switching transients, nor too small, to avoid frequent unnecessary disconnects. The initial set of monitor thresholds should be based on computer analysis/simulation. Optimization and final adjustment of threshold settings should be performed during flight test.

-Appropriate methods should be considered to achieve smooth transition when switching from full system configuration to less than full configuration, which includes reduction of levels of redundancy that result only in a reduction of AFC integrity levels, and cases that result in a reduction of flight control quality.

-AFC systems typically employ reset features to re-engage compromised parts of the AFC system, after failures, i.e., to re-engage one or more of several control paths that have been disengaged following a monitor trip, in case the condition that caused the monitor trip does not remain valid. These reset features may be automatic or manual and both of these types of reset features have specific safety concerns associated with them. Some of the concerns associated with the automatic features include determination of all appropriate conditions for reset, and determination of all appropriate conditions to inhibit reset. Some of the concerns associated with manual reset include crew workload, and the ability of the crew to determine appropriate conditions for reset actuation. Detailed procedures to use this feature must be established and approved, and it should incorporate protection mechanisms to avoid flight hazards, if incorrectly engaged.

(2) Robust Design

A system that employs robust design may independently be able to reduce the effect of failures to a level consistent with its failure classification. While redundancy management is an active method of failure compensation that consists of system monitoring, fault detection, system reconfiguration, and failure state indication, a system with robust elements may remain passive at the occurrence of a failure. Fault tolerance may be accomplished by redundant components and/or protective devices, with possibly some aspects of robust design.

Robust design features are usually applied as a complementary solution to continuous monitoring and redundancy management.

Typical robustness features are:

- Redundant components
- Filters
- Signal limiters
- Signal averaging

Examples of considerations of fault tolerance practices to be achieved for robust designs are:

-Switches with redundant electrical contacts can be switched to the ON position (conduct) with one pair of contacts being failed open circuit and, respectively, to the OFF position (interrupt) with one pair of contacts failed closed circuit.

-Annunciators with redundant incandescent bulbs remain functioning after failure of one bulb.

-Buffer batteries that are diode isolated from the primary electrical power supply provide continuous electrical power in case of interrupts of the primary power source.

-Tandem actuators with redundant hydraulic pressure supplies remain operational after a hydraulic power failure.

-Filters (e.g., noise filters, notch filters, anti-aliasing filters, phase compensation filters) protect the system from signal disturbances, structural coupling, oscillatory failures, and pilot-induced oscillations.

-Signal limiters prevent dangerous commands from getting through to the actuators.

-Fault tolerant consolidation of the output signals from a multiple channel system (e.g., non-linear signal averaging) is able to compensate for a runaway of one channel.

Failure effects of AFC elements used in a robust design relating to system functions are:

-Failures of parallel redundant components typically are not automatically detected and indicated, and therefore remain in the system as latent faults. A subsequent failure of the corresponding component results in a functional failure.

-After failure of filters or signal limiters, the protective function of these elements is lost. Such failures typically are not automatically detected and indicated and therefore remain in the system as latent faults.

-Buffer batteries with low capacity may not provide sufficient electrical power to keep the system operational in case of emergency.

Examples of considerations of design practices to maintain the safety functions of the AFC to be used in a robust design:

-Redundant components must be individually tested. Internal test points should be provided to get access to these components, if some type of Built-in Test (BIT) feature does not check them. The tests should be carried out on a regular basis to limit the period of latency of potential latent faults. The SSA determines the allowable time between the tests.

-Filters and limiters, if provided by hardware, should be tested on a regular basis to limit the period of latency of potential latent faults. The SSA determines the allowable time between the tests.

-The capacity of buffer batteries should be regularly checked to keep the batteries in good condition.

(9) Validation of Pilot-Vehicle Interface Assumptions

The SSA on the developed system should validate the pilot-vehicle interface assumptions made in the FHA. When addressing the validity of these assumptions, the following considerations need to be taken into account.

AFC System Controls, Status, and Warning and Caution Indications.

Flight Manual Instructions.

Training for flight with degraded HQs if the level of degradation results in diminished control characteristic demands pilot training.

The validity of the assumptions should be proven using a means of assessment that is appropriate to the consequences of the failure.

The more severe the consequence of the failure or assumed increased pilot action, the greater the rigor required for the validation of the assumption. Techniques to validate these assumptions, as a part of the SSA, may include analysis, simulation, modeling, ground, or flight test, as appropriate.

For example:

Status, Warning, and Caution systems should be evaluated with a clear understanding of the functioning and failure effects of the AFC. Evaluations should include ground and flight assessments with normal and emergency use in representative operational situations. Other failures, e.g., electrical system failures, which can affect the AFC, should also be evaluated, as supporting systems. Judgments should be made about whether the pilot can be expected to easily assimilate the status of the system(s).

The Flight Manual instructions and drills associated with normal and emergency operation of the AFC should be assessed in flight or on the ground in representative operational situations. The ability of the crew, particularly for single pilot operation, to follow the flight manual procedures should be determined given that the flight characteristics could be degraded and should not require excessive workload or skill.

Failures to be evaluated depend upon the architecture of the particular AFC system design under consideration while the FHA provides information on the failure probabilities and hazard classifications. The following failures that may affect the AFC are indicative of the type of failures that may have to be considered:

- Hydraulic system failure effects
- Electrical power system failure effects
- Common mode failure effects
- Loss of redundancy
- Loss of sensor and interface failures including data busses
- Loss of indications to the crew
- Engine failures, including total loss of power

Trim and force-feel system failures
AFC warning and indicating system failures
AFC failures resulting in:

- Reduced stability
- Reduced control margins
- Reduced maneuvering capability
- Significant flight path discontinuities
- Pilot requirement to manually reconfigure the AFC system
- Automatic mode change failures
- Changes to inceptor characteristics

Evaluation of failure modes for which credit is sought for pilot action should be carried out to assess their characteristics. This would normally include failures classified as Minor, Major or Hazardous/Severe-Major as defined in AC 29.1309. The purpose of this assessment is to judge the overall acceptability of the piloting task and therefore validate if it is reasonable to expect the crew to carry out the piloting tasks assumed in the PSSA. The means of assessment should be agreed with the certification agency and may include a combination of quantitative and qualitative criteria for the degraded mode flight characteristics. There should be a methodology established to provide the relationship of pilot workload to the criticality of failures. For conventional stability augmentation systems this has been achieved by showing compliance with some parts of Subpart B flight requirements for VFR and within a practical flight envelope for IFR operations. The compliance to Subpart B is typically shown by analysis/simulation and selected tests to verify/validate the analysis/simulation. The number and type of tests are typically predicated on a case-to-case determination, based on AFC architecture, and rotorcraft performance and flight characteristics. These include both quantitative and qualitative requirements. If the characteristics of the normal operation of an AFC System require special conditions to show equivalence to the quantitative requirements of Subpart B, the relevant parts of the special conditions would also apply to the failure cases identified above. The method for evaluating the handling qualities of the rotorcraft should be agreed between the applicant and the authority as a specific guidance material.

(10) Evaluation Methodology

The performance of AFC systems, as for conventional flight control systems, should be evaluated to demonstrate that the safety requirements are met under all failure conditions. This is generally considered a part of the SSA activities. There are various evaluation methods available; some are listed as follows:

- Non-Real Time Computer Analysis
- Pilot-in-the-Loop Simulator Test
- Bench/Rig Test
- Rotorcraft Test
- Flight Testing

-Service History

For certification purposes, failures classified as major would normally be verified by flight test. The decision as to which failures should be tested should be made after determining which failures have an identifiably unique effect on the behavior of the aircraft. For example, it may be possible to group types of failures and then flight test the worst-case failure that covers that group or class of failures, and possibly test samples to prove the validity of the groupings. Identification of the appropriate tests will be based on analysis, bench and rig tests, piloted simulation, ground test, and development flight test results. This identification process must be rigorous to justify the reduced amount of flight-testing.

Failures classified as hazardous /severe-major are typically verified by use of simulation. However, some failures classified as hazardous/severe-major can also be efficiently and safely tested in flight. FHA hazard classifications are determined in relation to flight operation modes and flight phases. With carefully flown flight tests using typical flight test facilities, e.g., telemetry, safe altitude, incremental approach, flight modes/phases, a failure that has been determined to be hazardous may be safely evaluated by flight testing to evaluate these particular failure modes/phases. Normal flight test considerations of identifying the worst-case test conditions, e.g., weight, center of gravity, speed, rotor RPM, density altitude, etc., should be observed. Failures conditions classified as catastrophic should be verified by means other than flight-testing. There maybe a relationship between the levels of integrity provided to satisfy a determined failure condition category and the methodology used to validate the adequacy of the provided integrity. The table in the following figure addresses this relationship:

Failure Condition Categories	Suggested Methodology for Validation of Design Integrity			
	Provided Integrity Level			
	10 ⁻³	10 ⁻⁵	10 ⁻⁷	10 ⁻⁹
Minor	Possible Flight Testing Analysis (4)	Possible Flight Testing Simulation Analysis (4)	Simulation Analysis	Analysis
Major	N/A	Possible Flight Testing Simulation Analysis	Possible Flight Tests Simulation Analysis (1) (2)	Simulation Analysis
Hazardous/Severe-Major	N/A	N/A	Possible Limited Flight tests Simulation Analysis (1) (3)	Simulation Analysis
Catastrophic	N/A	N/A	N/A	Analysis (with possible simulation to validate analysis assumptions)

**Figure AC 29 MG 17-1
Validation Methodology**

(1) These shaded areas represent AFC validation methodology that might employ limited flight-testing. This should be determined on a case-to-case basis.

(2) Flight testing as a validating methodology, for this combination of provided integrity and failure condition categories may be minimized due to the design providing a level of integrity higher than the addressed failure condition category.

(3) Flight testing as a validating methodology, for this combination of provided integrity and failure condition category, should be minimized due to safety in testing considerations. However, flight-testing that is desirable may be feasible for some aspects if proper limitations are observed.

(4) For those probable failures evaluated as having minor effects, flight-testing is an option if the effects are not obvious, and/or if the closed loop effects can only be evaluated in flight, for analysis/verification.

AFC systems typically have a large number of test cases of single and multiple failures that should be investigated to verify the safety functions under all failure conditions, due to AFC inherent complexity.

(i) Non-Real Time Computer Analysis.

As indicated in Figure AC 29 MG 17-1 above, validation of AFC failures with a criticality classified as Hazardous/Severe-Major or Major may be performed by simulation or, respectively, flight test. At the beginning of the development process, when system components are not yet available in hardware, non-real time computer simulation is a useful tool for supporting the PSSA. This allows, at an early stage of the development, to predict the effects and assess the criticality of failure modes of the flight control system

(ii) Pilot-in-the-Loop Simulator Test.

It may be practical to use a Flight Simulator (FS) to qualitatively verify safety assessments for certain AFC failure conditions that would be high risk or unsafe to perform in flight. These assessments may be part of the SSA process used to show compliance with specific regulations. For example, the FS may be used to gather data on aircraft transients caused by a failure, crew recognition of the abnormal event, recoverability after the failure transient, and the ability to continue safe flight to landing after recovery. These assessments can be accomplished for critical, selected conditions using the FS without presenting a safety risk to the flight test aircraft.

(a) Test Environment

The test environment for pilot-in-the-loop simulator tests includes:

- Cockpit, equipped with AFC representative displays and controls
- Computer Generated Imagining (CGI)
- Simulated AFC system
- Simulated rotorcraft visuals and behavior

(b) Validation of Simulation Tools

Before final evaluation of failure mode effects using a Flight Simulator (FS), the FS should be validated for the specific test conditions identified in the test plan. This is especially required for failure modes that are either not able, nor advisable, to be evaluated in flight. Validation may be done quantitatively, qualitatively, or a combination of both. For example, a data package consisting of a quantitative comparison between flight data and simulator data can be provided for selected conditions to be evaluated to demonstrate the FS is suitable for the purpose of evaluating the failure modes. The FS integrity robustness is partly related to the safety margins contained in the AFC system

functions being evaluated. Mathematical models of the AFC system can be validated by bench test with hardware in the loop.

The flight simulator configuration, including hardware and software, should be controlled to ensure that the functional performance, as validated, is not corrupted during the certification process. The FS should be assessed to identify and preclude opportunities for misleading simulator results that could affect certification process and ultimately on the design of the AFC systems. Use of the FS should be assessed for functional criticality in relation to the effect that improper behavior of the FS may have on evaluation processes and ultimately on the design of AFC systems.

(c) Test Procedure and Expected Results.

The test procedure for pilot-in-the-loop simulator tests includes real-time simulation of performance with simulated failures. The expected test results are:

- Evaluation of pilot intervention time (recognition and reaction time) for the occurrence of failures under various flight conditions
- Assessment of Handling Qualities during recovery maneuvers
- Assessment of man-machine interface (controls and displays, warnings, cautions, and advisories)
- Evaluation of rotorcraft transients

(iii) Bench/Rig Test

One of the objectives of bench test and rig tests is demonstration and assessment of failure cases that are classified as Major to Hazardous/Severe-Major. The AFC system is installed in hardware, and tests are performed in either open loop or closed-loop configuration, where in the latter case, the rotorcraft is simulated by a mathematical model.

(a) Test Environment

The test environment for bench tests and rig tests includes:

- AFC system to be installed in hardware
- AFC system environment: to be as realistic as possible to simulate aircraft conditions, including mechanical installation of equipment, wiring, cooling, electrical and hydraulic power supplies, cockpit controls and displays, trim system, actuation system, actuator loads
- Rotorcraft to be simulated by a mathematical model (only required for closed-loop simulation)

(b) Test Procedure and Expected Results

The test procedure for bench tests and rig tests includes open loop and closed-loop tests with simulated failures.

The expected results are:

- Verification of failure logic, failure management, and resultant degraded modes
- Evaluation of transients during and after failure modes

Compared to validation of failure management in the simulator, the use of hardware-in-the-loop simulation provides more realistic results with respect to signal accuracy and resolution, phase delay, and other hardware/software related effects.

(iv) Rotorcraft Test

Ground Test: Verification of some aspects of the AFC functionality should be possible on the ground, such as determination of stuck or jammed controls/actuators. Ground testing should be performed to check the safety functions with the equipment installed in the aircraft. Operation tests are performed to demonstrate that the flight control system is free from jamming. Limit load static tests are performed to demonstrate compliance with limit load requirements.

Flight Test: The objective of flight tests is to show compliance with the safety requirements and to validate assumptions for those objectives that cannot be tested on ground. Certain effects can only be addressed in flight, such as air resonance, structural coupling, and pilot-induced oscillations. Flight tests are carried out at various flight conditions without and with simulated failures. Rotorcraft performance and handling qualities are assessed under normal and failure operating conditions. Stimulation of the aircraft with simulated failures must be conducted without endangering the aircraft. This implies that the test conditions must provide for failures to be reset at any time to return to the faultless system configuration, if necessary.

(v) Service History

Meaningful information for a new design of an AFC system may be obtained from service history, such as verification of assumptions of failure probability figures, evaluation of failures occurring under operational conditions, and collection of recommendations from service pilots,

(D) Process Management

(1) Quality Control

Products are subject to quality controls processes throughout their service life, which means, design, manufacturing, installation, and maintenance activities. Traceability of relevant material batches or serialized items should be ensured and all changes in

suppliers, manufacturing, testing, or operations should be evaluated, documented, and dated.

Some mechanical parts or electrical parts may be considered critical for various reasons. Mechanical parts may be critical because they exist in a single load path for AFC applications. Electrical parts may be critical because of the possibility of a design, manufacturing, installation, or maintenance error simultaneously affecting redundant components resulting in catastrophic effects. Quality control procedures should continue throughout the production life cycle of AFC systems to minimize the possibility of common mode failures for critical parts.

Another consideration for critical electrical parts is the possibility of common mode failure caused by redundant components simultaneously reaching operational life limits. For example, electrically erasable memory devices may have manufacturer limits on read/write cycles of individual memory locations. For critical AFC functions, additional analyses should be performed to assure these types of parts are not susceptible to common mode failure throughout their production life cycle. Considerations of a service life should be addressed for the parts of the AFC whose failure could result in an unsafe operational condition.

Additionally, electronic control assemblies of an AFC system, that are the result of the aforementioned electrical parts and any manufacturing processes or materials should have sufficient quality control applied, to prevent the introduction of common mode failures being introduced into the AFC system's production cycle.

As a minimum, acceptance test and burn-in test should be performed on the electronic control assembly.

(2) Configuration Management

A configuration management process for AFC systems has no special considerations beyond that of a non-AFC system.

(3) Continued Airworthiness Requirements

To minimize the occurrence of latent failures for parts of the AFC design that may fail without detection, periodic checks and or inspections (in flight or on ground) may be required. These types of latent failures may result in reduction of required integrity levels. These latent failures in combination with one or more detected failure could result in a Hazardous/Sever-Major or catastrophic event. AFC systems should be subject to safety objectives evaluation from which the check or inspection periods are established. AFC designs should minimize the reliance for Certification Maintenance Requirements (CMRs) to compensate for AFC integrity shortfalls (reference AC 29-2C, Change 1, paragraph AC 29.1309b(4)(v)(D).) Other considerations are for replacement parts throughout the life of the AFC system. A parts screening process should be a part

of the type design to prevent a decrease in parts surveillance for critical aspects of the AFC system.

SECTION 2

(2) Certification Guidance for Specific Rules Addressed by Safety Assessment

While conducting the Safety Assessment process on AFC systems, careful attention should be given to those FAR/JAR sections that, either due to the application of new technology or designs, may be candidates for special conditions. This MG provides guidance on the following FAR/JARs as they apply to AFC systems.

(i) Reference to §§ 29.671(a) and (b), Control Systems - General

(A) Introduction. Transmission of control inputs to rotors, for conventional rotorcraft controls, were made through mechanical or electro/hydro mechanical devices. Determination of the origin of perturbations to signal transmission was relatively straightforward since failure cases could usually be classified in a limited number of categories, such as: maintenance error, jamming, disconnection or failure of mechanical or electromechanical elements, structural failure of hydraulic components, or failure of supporting systems. However, for AFC systems, the transmissions of control inputs are submitted to many threats different from those expected on mechanical parts.

In AFC Systems, spurious signals coupling into the command signal loop may lead to unacceptable system response. The resultant system malfunctions could cause system instabilities and the loss or freeze-up of functions may lead to a lack of system response, with flight hazards consequences. It is imperative that the command signal remains continuous and free of internal and external perturbations and common cause failures. Therefore, special design measures should be employed to maintain AFC systems integrity levels to meet the same level of safety, at least, equivalent to that which is achieved with traditional hydro-mechanical designs. These special design measures can be monitored through the SA process, provided specific care is put on AFC development methods and on quantitative and qualitative demonstrations of compliance.

(B) Conclusion: For the AFC aspects discussed above, the SA process as addressed in Section 1 of this document is a sufficient means to show compliance to this paragraph. There is no need for a special condition because, problems occurring in such systems are generic in nature and may be addressed the same as for those of any other electronic system. The mechanical aspects that relate to §§ 29.671 (a) and (b) can be addressed as stated by the guidance provided for § 29.695, Power Boost and Power Operated Control System, in paragraph iv below.

(ii) Reference to § 29.671(c) Control Systems - General

(A) Introduction. One intent of this paragraph is to ensure that full control is available before flight, without impediment. With AFC systems there is no direct physical relationship between pilot inceptors and rotor controls. Therefore reasonable assurance for full control availability cannot be accomplished by simple means as for flight mechanical controls. Additionally, SA alone cannot demonstrate that full authority will be available before flight. Pre-flight tests are necessary to demonstrate, as a minimum, that inceptors and actuators controls are free from jams and foreign objects. These preflight tests may consist of combinations of actual rotorcraft control initiated tests, AFC built-in tests, and maintenance checks/tests. Some of the considerations for these methods of assurance are as follows:

-Automatic pre-flight BIT (Pre-Flight Built-In Test) will be performed with limited authorities due to possible dangerous wind conditions and possible rotor limitations

-The pilot may perform a more complete inceptor stroke check when allowed by acceptable conditions (clearance, hydraulics available, etc.).

-Maintenance action should be able to check:

- Full actuator strokes
- Full inceptor strokes

-Functional ability should be demonstrated for the system's ability to reconfigure and continuity from inceptor to blades must be assured for all available redundancies

A check of full authority for all configurations prior to flight may not be practical to implement, due to the number of redundancies and degraded configurations of a typical AFC system. Additionally, some types of aerodynamic control implementations may be damaged by static preflight full actuator motion. Some of the control implementations that warrant considerations for possible damage are rigid rotor systems and those that employ elastomerics.

(B) Conclusion. Section 29.671(c) requirement is stated as requiring "a means must be provided that will allow the pilot to determine that full control authority is available prior to flight." The determination of compliance may be a combination of Built-In-Tests (BIT) and pilot operation of the AFC systems. A special condition or an *equivalent level of safety finding*, to address the safety concerns of this paragraph, may be required depending upon the methodology employed to show compliance to the intent of this rule and the degree to which compliance to this rule can be shown.

(iii) Reference to §§ 29.672 (a) and (b), Stability Augmentation, Automatic, and Power Operated Systems

(A) Introduction.

Section 29.672 addresses failure management for Power-Operated Systems and addresses simplex system's failures, without consideration for mitigation by required

pilot interventions. Section 29.672(b) addresses when the pilot is required to intervene for failure events to avoid unsafe conditions by counteracting the failure and deactivating the failed power operated system.

This rule's paragraphs (a) and (b) as written did not envision multi-redundant AFC systems, with failure management features, where a large number of configurations are automatically selected after failure, and where pilot intervention is generally not required or is minimized. Section 29.672(a) states, "warning systems must not activate the control system," however, this requirement is incompatible with typical AFC implementations, in that the same mechanisms that activate warnings also typically activate compensations for the failure(s) in the flight controls. AFC systems should have the capability to recover lost functions automatically. Such capabilities are not addressed elsewhere within the present rules. With these AFC types of systems, performance with the associated crew information and procedures should be addressed within the scope of this paragraph.

(B) Conclusion. Section 29.672 (a) and (b) are not well adapted to AFC systems in terms of compliance criteria for configurations and modes associated with AFC systems that are implemented with high levels of redundancy, complex integration, and automatic re-configuration features. The intent of this paragraph is that rotorcraft are safely controllable, when any failure condition or malfunction occurs at any point within the approved flight envelope, or is controllable and maneuverable when degraded to a practical flight envelope identified in the flight manual. The SA process, as described in detail in Section 1 of this MG, should be employed as a means to show compliance to the basic intent of §§ 29.672 (a) and (b). That intent is that the occurrence of any failure condition that would prevent continued safe flight and landing must be extremely improbable. The SA process may also be used to prove that the probability of degradation to lower levels of handling qualities due to AFC failures is compatible with the hazard classification.

A special condition for § 29.672 (a) and (b) may be required when applied to an AFC system.

(iv) Reference to § 29.672(c), Stability Augmentation, Automatic, and Power Operated Systems

(A) Introduction.

Section 29.672(c) addresses Stability Augmentation, Automatic, and Power Operated Systems in relation to a single failure. For SAS system failures in relation to evaluation considerations, refer to Section 1 of this guidance, "Validation of Pilot Vehicle Assumptions." However, for the single failure considerations of AFC systems that are provided as either a primary or sub-mode function(s) refer to Section 1, "Bottom up Analysis," of this guidance.

(B) Conclusion. Section 29.672(c) is not well adapted to AFC type systems. This paragraph was written to address SAS, automatic, and power operated systems from the aspect that these were enhancements to traditional mechanical controls, not the type of flight controls. AFC systems are typically power-operated controls with automatic, and SAS features. Therefore, the single failure concept addressed by this rule will need to be addressed at the highest command implementation level, to assure the safety considerations implied by this rule. Because of the need to apply the single failure concept to the AFC at the command level, this rule is a candidate for a special condition.

(iv) Reference § 29.695 Power Boost and Power Operated Control System.

(A) Introduction. This rule's importance to AFC systems, for the most part, is associated with the need for the hydraulic system as a supporting system for the AFC. As a supporting system for AFC systems, this rule as written, may not adequately support the safety goals determined by the AFC safety assessment process. (Refer to AC29-2C change 1, MG13 for Supporting Systems.)

As a supporting system to AFC systems, hydraulic systems need careful consideration and assessment for both their ability to perform power-assisted functions and to receive control input from AFC systems. This rule as written applies to the hydraulic/mechanical portions of the hydraulic system, but does not address considerations for non-mechanical control inputs.

(B) Conclusion. Both quantitative and qualitative aspects of the SA process should be applied to the AFC system with the consideration that the hydraulic system is a supporting system. This rule may be a candidate for a Special Condition, depending upon the design implementation and the SA results while treating Power Boost and Power Operated Control System as a supporting system for the AFC. The safety level as determined by the SA shall be maintained; however, there may be other possibilities (e.g. CMRs, service history, alternate control means) that could consist of combinations of designed integrity with alternative means, and/or mitigating factors, to show compliance with this rule as associated with hydraulic systems.

(v) Reference to § 29.1309, Equipment, Systems, and Installations.

(A) Introduction. Existing § 29.1309 requirements for CAT A certification approvals are sufficient for AFC system because they contain requirements to address failures that prevent continued safe flight and landing, where § 29.1309 CAT B requirements do not. From an AFC systems safety level requirements standpoint, in relation to § 29.1309, there are no differences between CAT A and CAT B.

(B) Conclusion. Existing § 29.1309 requirements for CAT A are sufficient to meet AFC safety objectives. When proposing an AFC system in a CAT B, VFR rotorcraft, a special condition is required. The special condition should establish that

any AFC failure not shown to be extremely improbable must not prevent continued safe flight and landing.

(vi) Reference to § 29.1329 Automatic Pilot System.

(A) Introduction.

The requirements for this rule were based upon an autopilot system, with limited authority, to provide “hands-off” attitude or flight path hold functions. Specific requirements include the pilot’s ability to “override” the autopilot to control the rotorcraft and have a means to disengage the autopilot by each pilot. This rule addresses the requirements for an autopilot that cannot produce hazardous deviations to the flight path under normal or failure conditions. A showing of compliance to these requirements results in extensive testing of “induced fault signals” into the autopilot during development and certification. Specific guidance material was developed to standardize the appropriate delay times prior to pilot actions to correct the failure, based on flight conditions. Compliance with these delay times dictated the design of the autopilot system in many rotorcraft.

The implementation of an automatic pilot system using AFC designs could be similar to present technology with a limited authority to provide the hands-off rotorcraft control, or may use control laws within the AFC to provide these functions.

(B) Conclusion.

The application of AFC technology typically provides full authority for classical autopilot functions and includes additional tailoring of the control laws to optimize performance of specific missions/tasks. Tailored modes of operation may significantly change the flight or operating characteristics of the rotorcraft and the present guidance material is inadequate to ensure that the required matrix of failure cases is evaluated. The assurance that these cases are addressed is contained in the SA process of Section 1 of this guidance.

The protection against unacceptable flight control behavior of either design configuration (Classical or AFC) is contained in the required safety objectives for the AFC basic features. This may make hardover evaluation envisioned by the existing rule unnecessary to show compliance.

For AFC systems, this rule is a candidate for a special condition or an equivalent level of safety finding to address the required systems/crew interaction differences with existing autopilot systems.

(vii) Reference to § 29.1351, General, and § 29.1355, Distribution System.

(A) Introduction. The importance of these two rules to the AFC system is, for the most part, associated with the need for the electrical power generation

(§ 29.1351) and distribution systems (§ 29.1355) of an aircraft to be considered as a supporting system for the AFC. As a supporting system for the AFC system, this rule as written may not adequately support the AFC safety assessment process for FAR 29 Category A and B approvals.

As a supporting system to AFC systems, electrical power generation and distribution systems need careful consideration and assessment for both its ability to generate and distribute electrical power to the AFC system. This rule, as written, addresses traditional aircraft power generation and distribution systems for aircraft systems (e.g., FMS, Avionic Displays, Autopilots, etc.) that rely on the aircraft's electrical generators and/or aircraft emergency battery. For AFC systems, it is envisioned that most AFC systems will have some portions of their need for electrical power provided by AFC dedicated electrical power sources (e.g., PMG); therefore, §§ 29.1351 and 29.1355 will need to be re-evaluated, for overall electrical power requirements and for AFC applications. AFC systems would require independence for electrical generation and transient considerations that are not adequate by existing rules.

(B) Conclusion. Both quantitative and qualitative aspects of the SA process should be applied to the AFC system with the consideration that the electrical power generation and distribution system is a supporting system. This rule is a candidate for a special condition, because the present rule does not adequately address the electrical generation and distribution system for Category A and Category B approvals that would be acceptable for AFC systems.

(viii) Reference to FAR 29, Appendix B, Airworthiness Criteria.

(A) Introduction. The existing Appendix B defines the additional requirements for certification of rotorcraft to be eligible for IFR operation. These requirements did not envision the design of AFC systems. AFC guidance on flight characteristics requirements of Appendix B is found in Section 3 of this guidance, "Certification Guidance for Rules Not Addressed Specifically by the Safety Assessment." The remaining issues applicable to AFCs found in Appendix B are for the categories as follows:

Stability Augmentation Systems (SAS)
Equipment, Systems, and Installation
Miscellaneous Requirements

For SAS system failures, refer to Section 1 of this guidance, "Validation of Pilot Vehicle Assumptions."

Another category of IFR requirements contained in Appendix B is Equipment, Systems, and Installation. This category is divided in to two subcategories. One subcategory is requirements for Flight and Navigation Instruments. This subcategory is, in theory, independent of AFC systems. However, there may be designs that integrate flight and navigation display systems with AFC systems. The SA process would evaluate these

types of designs; the resulting safety goals may not be adequately addressed by this subcategory.

The other subcategory is Miscellaneous Requirements. This subcategory addresses the requirements for instrument systems and other systems essential for IFR flight. These requirements address ice protection, adequacy of electrical power, or any other type of power that support these types of instruments and systems essential for IFR flight. Additionally, this subcategory addresses the isolation requirements that are a part of the concerns for fault tolerance, and ultimately the integrity requirements for these types of systems. The icing and power adequacy parts of the rule are sufficient for AFC systems. However, the isolation requirements for flight instruments for crewmembers were not written envisioning AFC type systems that are inherently highly integrated. With this integration, it may not be possible to meet these isolation requirements, and integrity requirements may have to address these safety considerations instead. These integrity requirements need to be a result of the SA determined safety goals.

The last two categories of IFR requirements address Thunderstorm Lights and Rotorcraft Flight Manual. Neither of these categories needs different rules for AFC systems.

(B) Conclusion. The requirements contained in Appendix B, in part, do not address the type, and scope of integration typical of AFC systems. The Appendix B requirements that are unaffected by AFC systems are for Thunderstorm Lights and the Rotorcraft Flight Manual. Additionally, the ice protection and power adequacy portion of Miscellaneous Requirements are unaffected. The flight controls and their effects are candidates for special conditions due to their requirements being driven by the safety goals determined for the basic rotorcraft's AFC SA process. The flight instruments requirements contained in Appendix B may be a candidate for a special condition due to the integration aspects of the typical AFC system. The requirements for the flight instruments that address independence and the resultant isolation for fault purposes are candidates for special conditions, for the above stated reasons.

SECTION 3

(3) Certification Guidance for Rules Not Addressed Specifically by Safety Assessment.

(i) Introduction. This section provides guidance for compliance to those items of AFC that are not covered, either in part or totally, by the SA process. This guidance will identify those items that are addressed by present rules, partly addressed by present rules, not adequately addressed by present rules, or require new compliance methods. Guidance is provided on the intent of existing rules to assist in developing the content of special conditions that provide an equivalent level of safety.

(ii) Flight Characteristics (Subpart B and Appendix B).

These issues are addressed in the rules of FAR/JAR Subpart B and Appendix B. The intent of these rules is to define the minimum safety level for certification designs of VFR and IFR rotorcraft. Some of these rules address the design of the control characteristics (static stability requirements of § 29.143 are a typical example) only in terms of direct equivalence between stick motion and servo actuator motion. AFC laws typically do not have this direct equivalence between the stick motion and the servo-actuator motion (Translational Rate Command control law is a typical example). These “design-oriented” requirements are not appropriate for AFC systems that cannot show literal compliance to these rules. Special conditions may have to replace or supplement these rules until the rules can be written to accommodate AFC systems.

The present rules address VFR as basic requirements and IFR is addressed as an addition to the basic VFR requirements. These two categories should be evaluated for flying/handling qualities as basic VFR requirements with additional requirements for IFR, even if typical AFC systems will meet the most demanding requirements (IFR). Compliance must be shown for the various AFC normal modes and control laws (normal means not due to failure) in all intended design flight envelopes and operating conditions. Normal modes of the AFC handling qualities should continue to meet the intent of the conventional stability and control requirements. If the AFC system has novel characteristics that result in the specific details of the existing requirements becoming inadequate, the intent of the existing requirements should continue to be met through a Special Condition, and a suitable evaluation methodology to show equivalent safety must be proposed by the applicant. The handling qualities aspects of failures and degraded modes are discussed in Section 1, paragraph b.1 (iii)(C) (9) Validation of Pilot/Vehicle Interface Assumptions, which asks for consistency between the means of compliance and special conditions for normal and degraded mode handling qualities.

An AFC allows many possibilities for developing novel flight control laws. In the simplest form, an AFC could simply replace the function of a direct link between the flight controls and the swashplate. The handling qualities of the rotorcraft would then depend on conventional factors that the current flight requirements are intended to deal with. A more likely situation is that an AFC would be used to modify the relationship between control input and rotorcraft response. Development of these novel flight control laws will require alternate means of evaluation methodologies. For example, there has been a great deal of research into rotorcraft response types (e.g., ADS33--referenced in Section 1 for applicability of standards) which has resulted in concepts such as Rate Command/Attitude Hold (RCAH), Attitude Command/Attitude Hold (ACAH), Translational Rate Command (TRC), etc., where response types have been related to the intended operational situation in terms of visual cues.

There are broad parallels with the concept of higher stability requirements with degraded visual environments in the existing flight requirements, in that for VFR (broadly meaning good visual cues with orientation of the aircraft by external cues), there are minimal handling qualities requirements that could in general be satisfied by a rate command system, even without an attitude hold function. For IFR flight (broadly

meaning poor or no visual cues), attitude retention systems have been normal for Part 29 approval and single pilot Part 27 approval. For specialized operations, e.g., search and rescue, autopilots giving translational rate command characteristics have been developed and certificated.

AFC controls laws proposed for certification must be carefully developed bearing in mind the current accepted standards, and the response of the rotorcraft has to be shown to be appropriate and acceptable for its intended use. Appropriate Rotorcraft Flight Manual (RFM) information on the intended use of the system in relation to modes of operation and visual cueing should be provided.

Flying/handling qualities requirement in FAR/JAR 29 are of six categories, as follows:

- General requirements
- Controllability and maneuverability
- Static stability requirements
- Dynamic stability requirements
- Force feel and trim requirements
- Ground and water handling characteristics

Note: The first five categories should be evaluated for VFR and/or IFR operations.

In the following sections, when handling qualities issues are raised by AFC rules, it should be understood that this guidance is relevant for pilot in the loop cases (closed piloting loop) and not relevant for open loop piloting modes (use of conventional type autopilot upper modes or “bugs and buttons and switches”).

(A) General Requirements (§§ 29.141, 29.171, and Appendix B)

(1) VFR (§§ 29.141 and 29.171)

General requirements are defined in §§ 29.141 and 29.171. They are basic requirements that address flight conditions (including engine failures) under which the flight characteristic requirements shall be fulfilled. They also require that the rotorcraft be controllable with an acceptable pilot workload in the previously mentioned flight conditions and with transitions from one condition to any other condition. These requirements are so basic that they shall apply everywhere control laws are addressed.

Further clarification is as follows:

In paragraph § 29.141(a)(4); the sentence, “. . . attainable with the controls rigged in accordance with . . . tolerances” may depend on electronic components and sensors tolerances, in addition to conventional parts of the control system. Guidance in AC 29-2C, change 1, for this rule is applicable for AFC systems. In addition, the cumulative effect of tolerances of electronic components and sensors should be included in the

demonstration of controllability, maneuverability and stability. Acceptable means of compliance include analysis, ground testing, and flight-testing.

AC 29-2C, paragraph 29.171, indicates that specific flight evaluation should be carried out in turbulence if the stability of the aircraft is considered marginal. Classic means of static and dynamic stability assessment use pilot inputs at the controls to simulate turbulence. For an AFC system, high frequency modes may exist that cannot be effectively excited by pilot inputs alone. For these circumstances, there may be the need for greater reliance on testing in actual turbulence or use of test equipment to establish acceptable rotorcraft characteristics.

(2) IFR (Appendix B, Paragraph VII)

The existing HQ requirements are intended to address IMC flight conditions with respect to pilot workload. Specific requirements are concerned with the pilot's capability to control the rotorcraft during and after SAS failures (§ Appendix B, VII (a) and (b)). With traditional flight controls, SAS's (rate damping and/or attitude retention) were developed to meet Appendix B (IFR) flight characteristic requirements, although attitude retention systems are generally necessary to meet the full IFR stability requirements of Appendix B. The intent of the rule was to define minimum safety standards to address SAS failures not shown to be extremely improbable. For AFCs, the requirements for SAS in the current rules should be understood as consisting of only modes and/or control laws needed to achieve the Appendix B (IFR) flight characteristic requirements. For these, compliance with the existing requirements of paragraph VII remains valid, specifically that the characteristics of the AFC must not degrade (due to failures that are not extremely improbable) below those required to meet the Subpart B flight characteristics as required by Appendix B, paragraph VII (a)(2). Assessment of these failure conditions, that are not shown to be extremely improbable, should be consistent with the Safety Assessment process as proposed in section (b) (1) (iii) (C) (9) "Validation of Pilot-Vehicle Interface Assumptions" of this MG-17. Some control laws or modes, e.g., equivalent to upper modes such as Height Hold or ILS Coupling, may not be required for compliance with Appendix B flight characteristics. These modes must function appropriately in accordance with §§ 29.1301 and 29.1309, and must comply with the safety requirements of Appendix B, paragraph VII.

(B) Controllability and Maneuverability Requirements (§ 29.143)

(1) VFR (§ 29.143)

The controllability requirements of § 29.143 (a), (d) and (e)(1) are compatible with typical AFC systems. Most of the maneuverability requirements of § 29.143 (b), (c) and (e)(2) are not affected by AFC systems except for the control margins. The intent of the rule is to ensure that control margins (at the rotor and the anti-torque system level) are sufficient in the defined flight conditions to avoid loss of control, i.e., adequate control power exists to exit potentially hazardous flight conditions. The intent is also to provide the pilot with sufficient awareness of proximity to control limits, as was achieved with

conventional flight controls by the pilot's inherent awareness of cyclic stick and pedal position relative to control stops. For AFC systems, an alternate means of compliance may be required. For example, AFC systems incorporating automatic trim follow-up eliminate the direct relationship between control inceptor and cyclic or anti-torque blade pitch, so the pilot does not have physical awareness of control remaining.

The present guidance for the applicable parts § 29.143 may not be adequate for AFC systems in relation to pilot awareness issues and they may need to be addressed by special conditions. In order to meet the intent of these rules, control margins should be addressed at the rotor and anti-torque system level and considered for the issue of pilot awareness of control remaining, as limits are approached. The means of compliance (visual, auditory, or tactile cueing) must be effective during maneuvers typical to the type, especially during divided attention operations, and for representative environmental conditions. Full envelope evaluation is required to verify effective pilot cueing in flight regimes that exercise possible AFC design characteristics such as electronic control mixing, coupled stops, and dynamic authority limits.

It is especially important that failure effects of all parts of the AFC required for compliance with the controllability and maneuverability rules, e.g., a control margin indicating system, should be evaluated by the FHA to determine the failure condition category. Particularly, with an AFC system, compared to standard SAS, the first failure may not have an immediate perceptible effect on the flight characteristic or controllability of the rotorcraft. Following the first failure or combination of failures of which the pilot is aware, due either to rotorcraft behaviours or annunciations; possible subsequent failures may result in a reduction in the safe flight envelope of the rotorcraft. Hovering with cross or tail winds should be particularly considered because in these conditions credit for reducing the wind envelope may not always be taken as it may not be possible to maneuver the aircraft to mitigate the effects of the failure due to the proximity of obstacles. It must be shown that when hovering with cross or tail wind, for any failure condition which is not shown to be extremely improbable, the 17 knots wind speed controllability envelope or the approved low speed controllability envelope (if greater) can continue to be achieved. However, if a first failure occurs during another flight regime, (e.g. in the cruise) it could be acceptable for the 17 knots wind speed controllability envelope or the approved low speed controllability envelope (if greater) to be reduced. This reduced safe controllability envelope appropriate to the type of approved operation can be defined, if the first failure is detected, annunciated, and sufficient information is provided in the flight manual to define this reduced envelope. This prepares for potential subsequent failures that should be considered as a result of the SSA or to reduce workload.

The current AC material (AC 29.672(a)(2) and AC 29 Appendix B (b)(6)(ii)) deals adequately with the reduced flight envelope following failures in other parts of the flight envelope.

(2) IFR (no specific IFR paragraph)

There are no specific additional controllability requirements for IFR in Appendix B. The existing VFR controllability requirements remain relevant for AFCs, as previously addressed.

(C) Trim (§ 29.161)

(1) VFR (§ 29.161)

The rule in § 29.161 requires that (a) the longitudinal, lateral, and collective control forces be trimmed to zero in level flight at any appropriate speed; and (b) that there must be no undesirable discontinuities in control force gradients.

The intent of this rule is to (a) reduce physical demand in order to maintain a given flight condition, and (b) to allow release of the cyclic and collective controls for brief periods.

One purpose for the installation of an AFC will be to reduce pilot workload; therefore, the intent of this rule can be easily achieved with proper selection of control laws. However, the control forces may not be trimmed to zero with the application of some AFC laws.

The AFC methodology selected will determine if the present rule is adequate, or whether special conditions and/or AC guidance will be required.

AFC systems typically provide flight envelope protection functions that may or may not permit trimming the control forces to zero at airspeed outside the approved flight envelope. However, it is not the intent of the rule to require force to be trimmed to zero for speeds outside the approved flight envelope. For other aspects of envelope protection function, see paragraph (vi) of this section.

(2) IFR: (Appendix B, paragraph III)

The IFR requirement, for trim, is that it must be possible to trim the cyclic (longitudinal and lateral), collective, and directional control forces to zero throughout the IFR envelope.

The objectives of this IFR requirement differ slightly from VFR in that it must be possible to allow the controls to be unattended for a longer period of time.

The system must have a restoring moment back to the trim point if disturbed.

The control force (longitudinal) must vary with speed to provide a stick force clearly perceptible to the pilot.

The AFC selected design will determine if the present requirements are adequate, but many of the concepts developed will not comply with the present rules; special conditions to address trim will be required.

(D) Static Longitudinal Stability Requirements (§§ 29.173, 29.175, and Appendix B, paragraph IV).

(1) VFR (§§ 29.173 and 29.175)

The requirements defined in §§ 29.173 and 29.175, and 29.173(a) address the need to have a rotorcraft with intuitive piloting characteristics (push the stick to accelerate, pull the stick to decelerate). This requirement applies to AFC systems as well as conventional flight control systems. However, AFC systems may introduce speed envelope protection features that may prevent increase in speed with forward stick movement. In this case, compliance with § 29.173(a) would not be applicable, as it would require a speed increase beyond the approved flight envelope. A speed envelope protection system cannot prevent all speed exceedances, e.g., due to turbulence or upset maneuvers, so the requirement to test to $1.1 V_{ne}$ remains valid. Specific flight test means to override envelope protection will be required to demonstrate satisfactory characteristics to $1.1 V_{ne}$.

The rule, § 173(b) and (c), requires that slope of control position vs. airspeed, in general, be positive for airspeed conditions and flight regimes specified in § 29.175. This requirement is valid for advanced control systems using conventional control laws, i.e., systems that are based on a direct relationship between the cyclic position and the rotor actuator position. This requirement is not valid for AFC systems for which there is not always a direct relationship between the cyclic position and the rotor actuator position. In fact, the intent of the rule is to have a rotorcraft with a tendency to return to a speed datum after a disturbance. AFC systems using advanced control laws (e.g., ACAH, TRC) or inceptors may provide compensating features to the static longitudinal stability. A Special Condition should be developed to show that the rotorcraft exhibits suitable static and dynamic stability. The design objective is to ensure satisfactory characteristics in any condition normally encountered in service. A means of compliance should be provided to demonstrate that the AFC possesses satisfactory characteristics, at least equivalent to those achieved conventionally. Such means of compliance could possibly include a qualitative testing method that utilizes in-flight testing and/or suitable simulators.

Section 29.175 defines the airspeeds and flight regimes for which compliance to § 29.173 (b) and (c) is required. A complete demonstration for the whole-certified flight envelope is not practically feasible in flight tests. As a minimum, the flight regimes and airspeed defined in § 29.175 should be used for compliance demonstration by flight tests. There may be the need to carry out flight tests at additional speeds and conditions if the AFC automatically switches modes or control laws at defined points in the flight envelope.

(2) IFR (Appendix B, paragraph IV)

The requirements for IFR flight characteristics are defined in Appendix B, paragraph IV of the rule for FAR Parts 27 and 29, for typical flight regimes.

(i) General (Appendix B, paragraph IV (a))

Positive static control force stability is required for airspeeds and flight regimes specified in Appendix B, paragraph IV (b) to (f). The intent of this rule's subparagraphs is that any increase of the airspeed above the trim condition creates a positive force feedback to the pilot, and any decrease below the trim speed creates a negative force feedback. This will permit, in the short term, the pilot to feel any modification of the speed (i.e., flight path) when flying hands on.

There is also a requirement to return within 10% of the trim airspeed when the control force is slowly released. The intent of this rule is that the rotorcraft should return to near the datum airspeed when the stick is released and/or after disturbance. This characteristic will result in lower workloads and ensure that the rotorcraft will remain within the approved IFR flight envelope. One key consequence of this rule is that a means must be provided to ensure that a secondary pilot action (e.g., beep trim or trim release) is required to modify the long-term rotorcraft speed or attitude datum.

Any change to these two basic requirements (e.g., for AFC systems that supply automatic trim follow up related to this rule) will require a Special Condition.

(ii) Appendix B, paragraphs IV (b) to (f), define the airspeeds and flight regimes for which compliance with Appendix B, paragraph IV (a) is required.

A complete demonstration for the complete certified flight envelope is not practically feasible in flight tests. As a minimum, the flight regimes and airspeed defined in Appendix B, paragraph IV (b) to (f), should be used for compliance demonstration by flight tests. A means of compliance, acceptable to the FAA/AUTHORITY, should be developed as part of the Special Condition to demonstrate adequately that the AFC has satisfactory characteristics, at least equivalent to those achieved conventionally. Therefore, this rule is a candidate for Special Condition for AFC. There may be the need to carry out flight tests at additional speeds and conditions, if the AFC automatically switches modes or control laws at defined points in the flight envelope.

(E) Static Directional Stability (§ 29.177 and Appendix B, paragraph V(a))

(1) VFR (§ 29.177).

Section 29.177 requires that directional static stability be positive when collective controls and throttles are held constant in typical trim conditions defined in §§ 29.175 (a), (b) and (c). The rule also requires that sideslip increases steadily with directional control deflection for sideslip angles up to +/- 10° from trim. The rule also requires that sufficient cues accompany sideslip to alert the pilot when approaching sideslip limits.

The objectives of the rule are to provide the designs that allow for the pilot to maintain sideslip within the limits and to have a predictable response to directional control inputs for sideslip in forward flight. On rotorcraft with a conventional Flight Control System (FCS), this is provided by positive weathercock stability and adequate cues of the rotorcraft flight condition. These cues are currently provided by control displacement and other indications of side force. These cues may be different or missing for AFC systems.

It should be noted that the low speed regime is not addressed by § 29.175 (typical trim conditions) or § 29.177. Unique low speed control laws and associated blending of laws should be carefully addressed. These basic issues remain relevant, and an SC would be required to address requirements for any AFC with different characteristics.

(2) IFR (Appendix B paragraph V(a)). The rule in Appendix B paragraph V(a) requires: 1) static directional stability be positive throughout the approved range of airspeed, power and vertical speed; 2) in straight flight, the control position must increase in approximately constant proportion to angle of sideslip up to +/- 10° from trim; and, 3) at greater angles up to the maximum sideslip angle, any increase in the directional controls must provide increase in sideslip angle.

The objective of the rule for IFR is the same as VFR, but compliance to the rule is requested for the whole IFR flight envelope. For IFR low speed approaches, unique low speed control laws and associated blending of laws should be carefully addressed. Any change to these basic requirements will require a Special Condition.

(F) Static Lateral Stability (Appendix B, paragraph V (b))

(1) VFR: not relevant

(2) IFR (Appendix B, paragraph V(b))

The rule in Appendix B, paragraph V(b) requires:

- No negative dihedral effect for sideslip angles up to +/- 10° from trim throughout the approved range of airspeed, and vertical speed, except for a small area around trim.
- Longitudinal cyclic movement with sideslip must not be excessive
- For 'high' speed flight (above the low speed envelope), some positive lateral static stability (dihedral effect) has been the norm for IFR helicopters. This provides side force cues and avoids negative spiral stability.

The acceptability of a design that gives true zero lateral static stability should be investigated by a suitable means before committing to a design with this feature. A Special Condition may be needed.

For low speed IFR flight (definition could include factors such as below typical current V_{mini} , flight on back side of drag curve or the speed at which control law blending occurs) the requirement currently in Appendix B, paragraph V(b) for cross control coupling or force coupling may not be relevant other than to ensure the avoidance of exceeding structural limits. A special condition may need to be developed to cover low speed IFR characteristics.

(G) Dynamic Stability (§ 29.181 and Appendix B, paragraph V(i))

(1) VFR (§ 29.181)

The § 29.181 requirements are for any short periods oscillation occurring at any speed from V_y to V_{ne} to be positively damped. This rule is applicable to AFC systems.

Nevertheless, rotorcraft with AFC systems may experience low amplitude, neutrally damped residual oscillations at the control effectors. Non-linear characteristics of control effectors (e.g., friction, free play, or AFC failure effects) may couple with the flight control system and yield closed-loop oscillations. These residual oscillations may be deemed acceptable and in compliance with § 29.181 provided that, the worst-case amplitude and frequency of the residual oscillations are shown to not degrade the pilot's ability to satisfactorily control the aircraft. Demonstration of residual oscillation effects should include the following:

Worst-case amplitude and frequency should be determined based on the full range speed, power, and weight conditions, including maneuvers.

Flight test to verify that the human factor effects (i.e., fatigue, workload, and motion sickness) of prolonged flight with residual oscillations are acceptable.

Analyses to prove that the residual oscillations do not adversely affect structural fatigue or damage tolerance.

Oscillations resulting from AFC failure conditions, not extremely improbable, must be shown to allow continued safe flight and landing without exceeding structural limits or adversely affecting the pilot's ability to safely control the rotorcraft, by analysis or test.

(2) IFR (Appendix B, paragraph VI)

Same considerations as for VFR above

(iii) Ground and Water Handling (Subpart B)

(A) General (§ 29.231)

Section 29.231 states: “The rotorcraft must have satisfactory ground and water handling characteristics, including freedom from uncontrollable tendencies in any condition expected in operation.” Other related requirements concerning ground and water handling are contained in §§ 29.143, 29.235, 29.239, and 29.241. AC 29-2C already provides explanation and procedures for these rules, but certain aspects of AFC systems require additional guidance. Specific areas for consideration include control mode transition between air and ground/water contact, and ground handling on slopes and in winds.

Full authority AFC systems typically require ground/fly state mode transitioning to allow acceptable control characteristics in both flight regimes. For example, some AFC systems with model following rate or attitude command functionality require that rate and attitude feedbacks be disabled with weight-on-wheels/weight on skid gear logic status. Additionally, the feed-forward control mechanization should be transitioned to the equivalent of direct gearing between the cockpit controller and the swashplate position. Satisfactory ground handling is then dependent on successful mode transition. Section 29.231, by extension, requires safe takeoff, landing, and ground and water maneuvering without excessive pilot workload. As such, the normal operation of the AFC system must be considered for compliance to this rule. The safety assessment process described in Section 1 of this MG should address applicable failed state operations. If water operation is an expected condition, then further special consideration is necessary to ensure compatibility between ground/water mode transitions and the means for sensing both regimes.

Aircraft operations on slopes and in winds must meet the intent of § 29.231 that the AFC system shall not result in uncontrollable tendencies due to the pilot’s inability to maintain desired trim state. AFC systems with unique trim multi-axis inceptors typically require the pilot to maintain force out of detent during ground operations if the ground state rotor neutral point does not trim external forces. Taxi in winds, startup and shutdown in winds, and slope operations are typical flight scenarios that must be considered for satisfactory compliance to this rule. Depending on implementation, this rule may be a candidate for special condition.

With regard to the ground state flight regimes, the safety implications of extended duration ground operations with non-trimmable stick forces should be considered. Although the existing rule (§ 29.161) does not specifically address trim control on the ground, conventional flight control systems have typically allowed trim forces to be zeroed on the ground, thus enabling unattended control capability. This rule is also a candidate for a special condition against § 29.231 and/or § 29.161.

(B) Ground Resonance (§ 29.241)

(1) VFR (§ 29.241)

Section 29.241 requires the rotorcraft to not have any dangerous tendency to oscillate on the ground with the rotor turning. Introduction of an AFC system may result in more complex ground resonance modes and may require more analysis than required for helicopters with conventional flight controls.

Rotorcraft with AFC systems should follow the procedures for demonstrating compliance to § 29.241 as described in AC 29-2C. The intent of these procedures is to thoroughly exercise the rotorcraft during takeoff and landings to cover the full range of parameters that can affect ground resonance. These procedures are necessary to ensure that any potential ground resonance is positively damped and does not introduce a dangerous ground oscillation with the rotor turning.

In addition to these procedures, rotorcraft with AFC systems present new considerations for evaluating ground resonance that include the following:

Biomechanical coupling between airframe dynamics and pilot controller can create a destabilizing resonance condition, depending on pilot gain.
Control law mode changing with ground contact sensors can affect ground resonance characteristics.
AFC failure conditions can affect ground resonance characteristics.

In order to show compliance with § 29.241 for AFC systems, the following procedures, as a minimum, should be performed in addition to the procedures specified in AC 29-2C, Change 1.

Resonance characteristics should be checked with varying pilot gains. This should be done by test and include more than one pilot.

Each AFC configuration or failure state that is susceptible to ground resonance should be evaluated by analysis or test.

The rotorcraft should be tested for ground resonance at power settings that intentionally puts the aircraft light on its landing gear.

- (2) IFR: not relevant
- (iv) Strength Requirements (Subpart C)
 - (A) Limit Pilot forces and torques (§ 29.397)

The intent of this requirement is to ensure adequate strength throughout the flight control system when considering the forces likely to be applied by a pilot. This requirement remains valid for conventional controls. The requirement also applies to the remaining mechanical parts of an AFC, particularly the control inceptors used by the pilot. If the flight control inceptors are of a novel design, e.g. side stick inceptors, different criteria may be justifiable, in which case a Special Condition should be raised.

(B) Dual Control Systems (29.399)

This requirement remains valid for AFC control systems.

(v) Personnel and Cargo Accommodations (Subpart D)

(A) Cockpit Controls (§ 29.777(a)(b))

These requirements are for controls to be conveniently located and arranged to prevent inadvertent operation or confusion. This clearly remains relevant for AFC cockpit controls.

(B) Motion and Effect of Controls (§ 29.779(a))

Section 29.779(a) calls for the Flight controls, including the collective pitch control, to operate with a sense of motion that corresponds to the effect on the rotorcraft. This basic requirement remains valid, for conventional rotorcraft. However, for some non-conventional rotorcraft that may have combined collective pitch and forward thrust, (e.g. tilt rotor) in to a single control, a special condition may be required. Careful consideration should be given to the case of dual controls when non-linked controls are being considered. This configuration can potentially result in no response to control inputs if both pilots make opposing inputs possibly allowed for AFC systems due to the reduced potential for feedback between pilots than would be the case for conventional controls. It is possible also that opposing inputs could be considered confusing in critical flight situations as dealt with by § 29.777 above. No requirement exists stipulating that dual controls must be mechanically linked, however this has always been the case and it would be possible to create mechanical dual controls that worked independently with the output summed to the flight control system, this has never been done. Fly-by-Wire systems have resulted in non-linked controls being implemented for large fixed wing transport aircraft, but there may not be direct read across when considering the types of operation carried out by civil rotorcraft. Rotorcraft will typically spend a much larger percentage of flight time being handled by both pilots, with a large variety of low and high gain tasks to be carried out. This may result in a higher potential for both pilots to operate the controls at the same time. Thus, creating a particular consideration for training to be carried out on the type with considerations for unexpected emergency maneuvering situations, in all cases. Conventional mechanically linked controls give a known and accepted level of feedback between pilots, but this may not be the case for unlinked systems. Any proposed system without conventional (mechanical) force and position coupling between dual flight controls would be considered novel and will require a Special Condition with appropriate justification to show equivalent safety to existing dual control systems for use in rotorcraft carrying out typical roles and tasks. Some exceptions may be possible if sufficient inceptor artificial feedback can be achieved by other than mechanical means.

(C) Ditching (§ 29.801). Section 29.801(b), (c), and (d) requires that the aircraft must have satisfactory ditching characteristics, if certification with ditching provisions is requested. This requirement remains valid for AFC, which should be shown to function satisfactorily during and after ditching for a period of time sufficient to allow safe emergency egress, which will usually include rotor shutdown. Given that a full authority electrical AFC may be more susceptible to adverse control characteristics or malfunction during emergency water landings than conventional mechanical systems with limited authority SAS, some additional considerations for an AFC are:

Aircraft and rotor stability during and after water landing without activation of normal ground/air mode switching, and also considering that aircraft attitude will be affected by water surface motion.

Adequate short term protection of AFC components against possible water contact that could, for example, induce control malfunctions that would prejudice completion of safe landing and egress.

(D) Emergency Evacuation (§ 29.803), and Flight Crew Emergency Exits (§ 29.805)

(1) Introduction

These rules require passenger and crew egress independent of the reasons that may result in impediments.

(2) Conclusion

Rules are sufficient; however, unique AFC features that may cause impediment to egress should be considered, for example, side stick controllers.

(v) Instruments; Installation (Subpart F)

(A) Flight Director Systems (§ 29.1335)

Mode Awareness

This rule requires that a means be provided to indicate, to the flight crew, its current flight director mode of operation, recognizing that the control mode switch position is not considered acceptable to meet this requirement. Since the AFC system may provide numerous operational modes tailored for specific missions or type of operations, these requirements must be considered applicable for AFC systems.

The application of AFC technology will likely include more tailoring of the control laws to optimize performance of specific missions/tasks. These modes of operation may significantly change the flight or operating characteristics of the rotorcraft; therefore, a means must be provided to indicate to the crew; the current mode of operation. If

selection of an incorrect mode could create a hazardous condition, either a “lockout” scheme, annunciation of incorrect mode selection, or if acceptable, limitations in the flight manual (§ 29.1583) that define the operational or environmental limits must be considered. Flight manual limitations acceptability is based on a variety of factors that should be determined on a case-to-case basis. The procedures necessary for the proper use of each AFC mode should be included in the normal procedure section of the flight manual (§ 29.1585).

If the AFC design allows automatic re-engagement of an operational mode with a different level of augmentation, then this mode transition should be subject to a discernable and unambiguous annunciation that ensures crew awareness. The probability and effects of mode annunciation failure and unannounced mode transition should be included in the SSA.

Application of this requirement may be sufficient for installation of an AFC system that provides the classical (flight director) modes, but special conditions may be required if “special” modes are provided that significantly modify the flight characteristics to optimize specific mission tasks.

(B) Flight Data Recorder (FDR) (§ 29.1459)

AFC systems on new commercial rotorcraft usually contain detailed information pertinent to the data collection requirements of FAR 135. FDRs are an invaluable diagnostic tool in incident investigations. With AFC systems, such as Fly-By-Wire, the pilot command inputs, actuator commands, actuator position, rotorcraft attitudes, rates, and accelerations, as well as operating states and failure conditions are available as high redundant measurements of actual rotorcraft operating states. The applicant should give careful design consideration for the flight control system to provide the appropriate data for recording on an FDR.

(vi) Rotorcraft Flight Manual (Subpart G)

(A) Training Considerations

Training is a methodology that may be used to mitigate the compliance requirements for AFC systems that may require more than normal pilot skills. Section 29.1581 requires that information necessary for safe operation of the aircraft, because of design, operating, or handling characteristics, must be included in the flight manual. The development of model specific training is normally not a certification task, but this general rule will be applicable for requiring special training, if determined to be necessary. This may become necessary, if AFC system complexity requires special training, or if specific crew training is required to ensure that crew action(s) assumed in the PSSA and evaluated in the SSA will be achieved. Specific crew training and knowledge that can be assumed if defined for purposes of mitigation could be helpful in achieving compliance objectives.

Specific model training identified during development, certification, or operational suitability testing can be ensured by requiring a Type Rating in the model, or by defining specific training requirements included in the flight manual. Provisions for an AFC training feature that would facilitate training for crew interaction in relation to degraded flight control modes should be considered when other methods are not practical or available. Also, training devices and/or simulators are recommended, and may be needed for training of complex systems or critical procedures, but the requirement for these systems are normally outside certification activity. Coordination between certification and operational/training organizations will be required to determine if special conditions are necessary to ensure that training meets the airworthiness requirements of a specific aircraft.

(vii) Issues not covered by existing Rules and AC Material

This section covers items not linked to or adequately addressed by existing requirements. They should therefore be considered as candidates for Special Conditions.

(A) System-Structure Interaction

Rotorcraft with AFC systems may contain control functions that affect the structural integrity of the rotorcraft. Examples include active load alleviation functions such as stability augmentation or vibration suppression systems, and envelope protection functions such as overspeed protection and /or maneuver limiting. In these instances, additional safety considerations are necessary to account for the effects of these systems, and their failures, on structural integrity. The effects of these systems on structural integrity, either directly or as a result of malfunctions, should be taken into account when demonstrating compliance to FAR 29 regulations in Subparts C and D.

(1) Active Load Alleviation

The following methodology and criteria can be used to ensure that active load alleviation functions of AFC systems provide an acceptable level of safety. These criteria address the direct structural consequences of the AFC responses and performance, for both normal and failure conditions, and should be considered as part of the overall System Safety Assessment. Depending on the specific characteristics of the rotorcraft, special conditions may be required.

- Performance During Normal Operation

Limit loads should be derived from the limit conditions specified in FAR 29, Subpart C, taking into account the behavior of the active load alleviation functions for the specified limit maneuver or gust condition. Design limit loads can be defined assuming the active load alleviation functions are operable.

In accordance with the safety assessment process, the probability of losing an active load alleviation function should be consistent with the aircraft effects for continued flight with the function inoperable. Considerations for making this determination include failure detection, crew alerting, and operating procedures to minimize the probability of exceeding limit loads with inoperable active load alleviation. The severity of the structural load response to gusts and limit maneuvers, with the load alleviation function inoperable, should also be considered during the safety assessment process. The intent of these criteria is to establish a means to ensure that the probability of exceeding a design limit load condition is no greater than for rotorcraft with similar flight characteristics that do not contain active control functions.

It should be demonstrated by analysis, simulation, and/or test that static structural strength satisfy limit load criteria for symmetrical and asymmetrical structural maneuvers specified in Subpart C using the final configuration and control laws of the active load alleviation functions.

- Failure Transients

Starting from 1-g level flight conditions in the normal flight envelope, a realistic scenario including pilot corrective actions, must be established to determine the loads at the time of failure and immediately after failure. The guidance material for SAS failures (AC29-2C, Appendix B, b(6)) may be helpful in defining appropriate pilot actions and time delays. Flight simulation may be used to evaluate control responses associated with pilot corrective action. It should be shown by analysis or test that the rotorcraft can withstand these loads multiplied by an appropriate safety factor. The appropriate safety factor should be approved by the certification authority and may be related to the probability of occurrence of the failure.

It should be demonstrated that the failure transient does not lead to divergence, control reversal, or other hazardous aircraft effects.

- Continued Flight in a Failure State

After considering all appropriate reconfigurations and flight limitations, the following structural criteria should be met for the continuation of flight after a single failure or combination of failures not extremely improbable of the active load alleviation functions:

The existence of any failure condition, not extremely improbable, during flight that could significantly affect the structural capability of the rotorcraft unless mitigated by suitable flight limitations, should be annunciated to the flight crew.

Failures of the system that result in sustained structural vibrations should be evaluated to ensure that the vibrations do not produce loads that could result in catastrophic failure, divergent dynamic effects, detrimental deformation of primary structure, or hazardous effects on the flight crew or passengers.

If a restricted flight envelope is prescribed in a failure state, then it should be shown that the restricted flight envelope provides for normal flight maneuvers and excursions resulting from normal atmospheric disturbances without exceeding structural limits.

It must be shown that system failure(s) do not result in a condition where a parameter is limited to such a reduced value that safe and controllable maneuvering is no longer possible.

(2) Envelope Protection

The following methodology and criteria can be used to ensure that envelope protection functions of AFC systems provide an acceptable level of safety.

Onset of the envelope protection functions should be demonstrated to be smooth, appropriate to the phase of flight and type of maneuver, and not conflict with the ability of the pilot to satisfactorily maneuver the rotorcraft.

If the envelope protection protection system provides an override capability, then the override function should be evaluated to ensure that inadvertent exceedance of limit loads is precluded. If the envelope limits are non-overridable, then emergency maneuverability should be evaluated at worst-case foreseeable conditions.

If a restricted flight envelope is prescribed in a failure state, then it should be shown that the restricted flight envelope provides for normal flight maneuvers and excursions resulting from normal atmospheric disturbance, and that minimum acceptable flight to reach a suitable landing site is achievable.

(B) Pilot Induced Oscillations (PIO)

Pilot Induced Oscillation is defined as sustained or uncontrollable aircraft oscillations resulting from the pilot's attempt to control the aircraft. Unique aspects of AFC systems demand special consideration of the following three main classifications of PIO:

(1) Category I - Linear Aircraft-Pilot Interactions - Category I PIO is characterized by closed loop dynamic instabilities within the normal (linear) operating region of pilot-aircraft interactions. Quantification of the attitude frequency response bandwidth and phase delay parameters, against appropriate design criteria (e.g., ADS-33), provides the key indicator to assess the acceptability of a control system relative to PIO tendencies. For digital fly-by-wire control systems, the phase delay parameter includes latencies resulting from computer frame rates, asynchronous processing, sensors transport delays, data-busses, and actuators. A rotorcraft free of PIO tendencies will avoid high frequency phase roll-off, which can be achieved by maximizing the attitude response frequency and minimizing the gain at the 180-degree attitude phase lag frequency.

(2) Category II – Quasi-Linear Aircraft-Pilot Interactions

Rapid control inputs during dynamic loop closures can lead to actuator rate saturation and control surface position limiting. A combination of sufficient control rate capability and acceptable gain attenuation at PIO frequencies is needed to avoid sudden phase lag in the aircraft response during closed loop tasks. AFC systems, in particular, can be susceptible to Category II PIO due to feed-forward command models that may demand high frequency control motion. Reduction in the feed-forward gain at PIO frequencies may minimize the control rate saturation. Additionally, phase compensation filtering is a method to reduce phase lag between pilot commands and actuator rate that may reduce the tendency for PIOs to occur. The aircraft should be evaluated for Category II PIO tendencies by conducting large amplitude stick inputs during compensatory tasks, e.g., high gain tracking tasks. Failed state, e.g., single stage operation of a dual stage actuator should also be addressed, where reduced actuator rate capability can increase PIO tendencies.

(3) Category III – Highly Non-Linear Aircraft-Pilot Interactions

Unique features can precipitate category III PIO in AFC systems, such as control law mode changes, automatic envelope protection systems, and system re-configuration logic. AFC designs should not be susceptible to non-linear characteristics that can lead to non-intuitive control inputs by the pilot to achieve a desired response. Identification of system non-linearities that can abruptly change control response characteristics, and evaluating these conditions in flight during compensatory tracking tasks is an acceptable means of showing compliance.

(C) Rotorcraft Integration of Advanced Flight Controls

With the introduction of AFC systems into commercial rotorcraft, there is a growing interdependence or interaction with other rotorcraft systems and the flight control system. Systems such as electrical power, air data systems, electronic flight displays, engine controls, and other utility systems may interact with advanced flight control systems in unintentional ways as designers attempt to integrate functionality to reduce costs and weight. Some likely system issues to consider include:

Functional interdependency

Separate controls vs. redundancy (e.g., twin engine controls)
Data source consistency between displays and controls

SECTION 4

(4) Summary of Rules/Special Condition Issue

The table below summarizes the guidance provided in this document for the existing certification rules and other safety issues that are candidates for special conditions for AFC systems.

Note: These references provide reasons for determination of special conditions and should be utilized to develop those special conditions for a specific design. It may be possible to identify the need for special conditions from a generic position, for some issues. However, the need and specifics of the required special conditions, for most issues, are design dependent and need to be developed on a case-to-case basis.

List of Existing Rules & AFC issues for Special Condition Considerations	Paragraph Reference in This Document (Note 1)	Other References Advisory Circular or Standards Guidance
29.143	§ b (3) (ii) (B) (1)	AC 29-2C Change 1
29.161	§ b (3) (ii) (C) (1)	AC 29-2C Change 1
29.173	§ b (3) (ii) (D) (1)	AC 29-2C Change 1
29.175	§ b (3) (ii) (D) (1)	AC 29-2C Change 1
29.177	§ b (3) (ii) (E) (1)	AC 29-2C Change 1
29.671 (a), (b)	§ b (2) (i)	AC 29-2C Change 1, ARP4761
29.671 (c)	§ b (2) (ii)	AC 29-2C Change 1
29.672 (a), (b)	§ b (2) (iii)	AC 29-2C Change 1
29.672 (c)	§ b (2) (iii)	AC 29-2C Change 1
29.695	§ b (2) (iv)	AC 29-2C Change 1
29.803	§ b (3) (vi)	AC 29-2C Change 1
29.805	§ b (3) (vi)	AC 29-2C Change 1
29.1309	§ b (2) (v)	AC 29-2C Change 1
29.1329	§ b (2) (vi)	AC 29-2C Change 1
29.1351	§ b (2) (vii)	AC 29-2C Change 1
29 Appendix B Section III	§ b (3) (ii) (C) (2)	AC 29-2C Change 1
29 Appendix B Section IV	§ b (3) (ii) (D) (2)	AC 29-2C Change 1
29 Appendix B Section V	§ b (3) (ii) (E) (2) and § b (3) (ii) (F) (2)	AC 29-2C Change 1
29. Appendix B Section VIII	§ b (2) (viii)	AC 29-2C Change 1