Preliminary Safety Assessment for the Sidestick Move from Autopilot Signals Function

ARTEM SAVELEV[1], EVGENY NERETIN[2]
dept. Aircraft system design
Moscow Aviation Institute
(National Research University)
125993, Moscow, Volokolamskoe shosse, 4
RUSSIA
[1]artemsaveliev@inbox.ru
[2]e.s.neretin@mai.ru

Abstract: The main purpose of civil aviation is economical, reliable and safe flight operations. To develop a modern aircraft, each aircraft system must contribute to efficiency, reliability and safety. One of the most important systems in an aircraft is a flight control system (fly-by-wire) and autopilot systems. A flight control system includes, among other things, pilot controls in the cockpit - yokes (Boeing) and sidesticks (Airbus, Irkut, Sukhoi). Sidesticks are currently a higher priority for the development of pilot controls in the cockpit due to increased ecomony compared to yokes. When using side sticks, a problem arose that was not found on tightly connected yokes - the lack of tactile feedback on the pilot flying actions of the pilot monitoring (with manual control of the aircraft) and the spatial position of the aircraft in both pilots (with automatic control of the aircraft). Among other things, this problem is associated with an increase in the number of hard landings. These problems affect flight safety. At the moment, the main way to solve these problems is the development and implementation of active sidesticks. Active sidesticks are not certified on any of the large civilian aircraft. The purpose of this work is to research the safety of The Sidestick Move from Autopilot Signals Function. The safety research methodology is carried out in accordance with the recommendations of SAE ARP 4761 and SAE ARP 4754A. As part of the work, a Functional Hazard Assessment, a preliminary Fault Tree Analysis and a Common Mode Analysis were performed. As a result, the required Functional Development Assurance Level and the Item Development Assurance Level (which perform this function) were determined. Quantitative requirements for the probability of failure conditions that satisfy CS-25 standards were also determined. Thus, the need for the introduction of active pilot controls in the flight control systems of perspective civilian aircraft was analyzed and the necessary measures were taken to ensure the safety of this function.

Key-Words: Active pilot controls, Safety Assessment, Functional Hazard Assessment, Automatic Flight Control System, Failure Tree Analysis, Flight Control System

1 Introduction

The main objective of the development of modern aircraft is to ensure flight safety. Despite all the increasing methods of automating the aircraft control process, the final decision-making remains with the flight crew at especially dangerous flight phases - takeoff and landing.

Traditionally, the flight crew has the ability to control the main aerodynamic surfaces (elevators in the longitudinal channel and ailerons in the lateral control channel) using pilot controls such as sidesticks or yokes. (Separately from the roll and pitch control channels pedal posts is using to control the rudder, but that are not the subject of this article.)

The sidesticks used on modern passenger liners (for example, on airplanes of Irkut, Airbus, Sukhoi [1, 2, 3]), unlike yokes (Boeing [4]), do not have a rigid coupling with deflected surfaces and each other. This entails an increase in the time taken to take control of the flight crew in case of automatic control system failures and when transferring priority from one sidestick to another. Delay in the transfer of control in the event of a failure can aggravate the situation, even to a catastrophic situation.

One of the promising directions for the development of control systems should be expected in the use of active sidesticks, which will provide tactile interaction between pilots and will allow to implement warning and restriction functions on handles [5]. The purpose of the article is to analyze the need for active sidesticks in modern civilian aircraft. Based on the identified disadvantages of the architecture of the Flight Control System and autopilot, a preliminary safety assessment of the function “Sidestick move from autopilot signals” is required. This preliminary safety assessment includes a Functional Hazard Assessment (FHA) and a Failure Tree Analysis (FTA). FHA in accordance with [10] gives a qualitative assessment of failures of the function in question. Based on the expected consequences of possible types of function failures, requirements are put forward for the required Function Development Assurance Level (FDAL) for the function development as indicated in [6]. The FTA is carried out to determine quantitative requirements for the probability of occurrence of failures of those components that perform this function. Also, the FTA formulates requirements for the Item Development Assurance Level (IDAL) for components [6]. The article includes the following sections:

- analysis of the classical Flight Control System and autopilot architecture with analysis of the emerging problems of such an architecture when using sidesticks instead of yokes;
- suggestion for solving the problem of lack of tactile information using the “Sidestick move from autopilot signals” function. Performing an FHA;
- Performing an FTA for the most critical failure of the “Sidestick move from autopilot signals” function.

The results of the article are the conclusion about the need for active pilot controls in perspective Flight Control Systems and autopilots, as well as safety requirements for this function: requirements for the probability of failures, requirements for the level of guarantee for the development of a function and components that perform this function.

2 Classical Control System Architecture

The classical architecture interfaces of the pilot, Automatic Flight Control System (AFCS) and Fly-by-wire System (FBW) to directly control the flight crew through side sticks through flight control computers to the actuators, and feedback is provided using the spatial position of the aircraft. The classic interaction architecture is shown in Fig. 1.

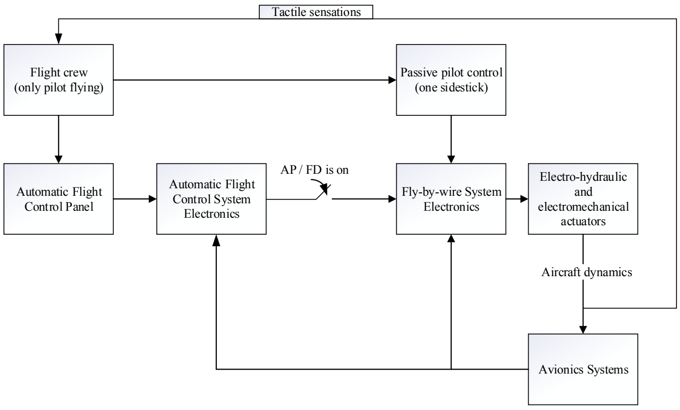

Fig. 1. Classical Control System architecture

This scheme allows the flight crew to interact with only one of the side sticks. Also, the pilot does not have tactile feedback on the sidestick position. This is a problem for autopilot failures in ICAO Category IIIb approaches.

The progress of automation in civil aviation leads to an increasingly frequent use of landings in categories ICAO IIIa and IIIb. The differences between the categories are shown in Fig. 2.

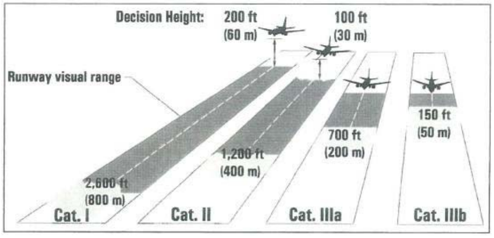

Fig. 2. ICAO approach categories

According to the requirements of CS 25.671(c), a delay of at least 4 seconds in the flight crew’s actions should be taken into account when failures occur before intervention in control (1 second for failure detection + 3 seconds for intervention in control). AFCS failures of the erroneous approach below 100 ft and above 50 ft with an automatic landing approach of category IIIb at an average vertical speed of 700-800 ft/min are possible. In this case, the height of increased attention will be crossed.

To avoid this situation, a reduction in the delay time is required. Active pilot controls will allow the flight crew to be directly in the aircraft control loop, without piloting on their own. Thus, the delay time before intervention in control can be reduced to 2 seconds (1 second for failure detection + 1 second for intervention in control). During this time, the flight crew will be able to determine the incorrect behavior of AFCS and make a decision to go around without crossing the height of increased attention.

The use of such methods of using the computing capabilities of modern FBW and AFCS will ensure the main goal of civilian flights - safety for passengers, flight crew and aircraft.

3 Perspective Control System Architecture

The perspective control system architecture implies the introduction of active pilot controls into the FBW and AFCS. With their help, the pilot will be able to use his sidestick to influence the movement of the second sidestick with manual control. It also opens up the possibility of using AFCS signals to move both sidesticks with autopilot control. The architecture of this interaction is shown in Fig. 3.

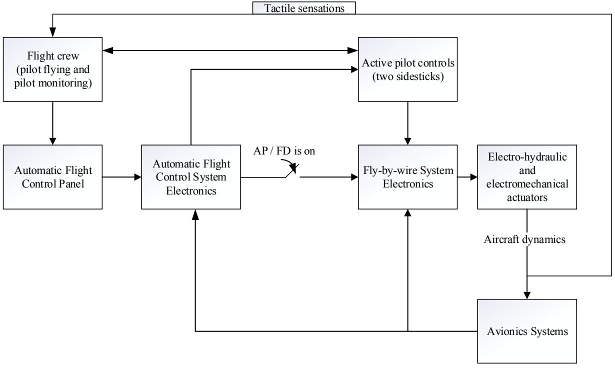

Fig. 3. Perspective Control System architecture

Such system architecture allows to provide the main hypothesis put forward in this article. Indeed, in this way, the flight crew will be directly in the aircraft control loop, even when controlled by autopilot. This should help to reduce the time before intervention in control in case of failures AFCS by half - instead of 4 seconds, it should be 2 seconds.

3.1 Preliminary Safety Assessment

The implementation of the interaction of active controls with an AFCS on real large aircrafts entails the introduction of a new sidestick move from autopilot signals function. In addition to the new functional requirements for software and hardware that require a set of measures in accordance with regulatory documents [6, 7, 8], a process of analysis and safety assessment of the implemented function should also be carried out [9, 10].

The first step in designing new functions in functional aircraft systems in the safety process is the FHA [11]. The purpose of FHA is to determine each type of function failure cases in question, their impact on the aircraft, crew and passengers, as well as to determine the criticality of these failure cases. Typically, the following two types of function failures require consideration: loss of a function (impossibility of its performance) and erroneous performance (non-compliance with requirements, spontaneous movement, etc.). The FHA results are FDAL for the function in question and requirements for the likelihood of failure occurrence. These requirements depend on the classification of failures by consequences.

The second step in a safety assessment process is the FTA. The main purpose of the FTA at the stage of forming safety requirements is to evaluate the proposed architecture of the function and the top-down components involved [12]. FTA is performed using the logical operators "AND" and "OR". The results of the FTA are quantitative requirements for the probability of failure of the respective components. FTA also allows to set the requirements for the IDAL for these components.

As know, in accordance with CS25.1309, no catastrophic failure condition should arise as a result of a single failure. In this regard, the third step of the safety assessment process is the formation of requirements to eliminate the common causes of failure (in the event that catastrophic failures are identified). This is part of the Common Mode Analysis. The main goal is to confirm that each “AND-event” (the parts of the Failure Tree obtained during the FTA connected by the logical operator “AND”) does not have hidden relationships that violate the independence of these failures. To ensure independence, ARP4761 provides a checklist that includes sources of common types of failure, such as concept and design (architecture, technology, materials, specification), production (manufacturer, procedures), assembly and installation (procedures), operation (personnel, procedures), maintenance (personnel, procedures), testing (personnel, procedures), calibration (personnel, procedures), external environment (chemical, electrical, radiation). Ensuring independence is possible only if independence is respected for each of these parameters.

These three steps are necessary to ensure that the safety requirements are complete and constitute the Preliminary Safety Assessment.

3.1.1 The sidestick move from autopilot signals function FHA

The applicable assumption for this FHA is the exclusion of the effect assessment on the passengers, because there is no direct interface between active pilot controls and passengers.

The main distinguishing feature of FHA is the assessment of function failures without taking into account its actual implementation in software, firmware and hardware.

The first type of failure condition that should be addressed by the FHA – Loss active sidestick tracking signals from AFCS.

The following assessment was carried out for failure condition “Loss active sidestick tracking signals from AFCS”:

- Aircraft impact - there is no effect on the aircraft, because this function is not currently implemented on aircrafts;
- Flight crew impact - the flight crew loses some information about the aircraft control. Continued safe flight and landing

Given the assessment of the failure impact on the aircraft and the flight crew, the maximum criticality corresponds to MINOR (MIN) due to a partial loss of crew awareness of the flight. MIN is classified as an insignificant situation. Allowable probability (qualitative assessment): probable event. Allowable probability (quantitative assessment): ≤10-3.

The second type of failure condition that should be addressed by the FHA - Erroneous active sidestick tracking signals from AFCS. With this function failure, it is impossible to say exactly how the flight crew will behave - it can interfere with control, but it can also ignore the incorrect behavior of the sidestick during the autopilot correct functioning.

The following assessment was carried out for the “Erroneous active sidestick tracking signals from AFCS” failure condition when the flight crew ignored the incorrect behavior of the sidestick:

- Aircraft impact - if the crew ignores the sidesticks incorrect behavior, there is no influence on the aircraft safety;
- Flight crew impact - the flight crew ignores the sidesticks incorrect behavior. If the need arises takes control or disables

Given the assessment of the failure impact on the aircraft and the flight crew when the flight crew ignores the incorrect behavior of the sidestick, the maximum criticality corresponds to MIN due to the presence of false information about the behavior of the aircraft through one of the available channels for determining the spatial position of the aircraft. As mentioned above, the following requirements meet this situation: allowable probability (qualitative assessment): probable event. Allowable probability (quantitative assessment): ≤10-3.

The following assessment was carried out for the “Erroneous active sidestick tracking signals from AFCS” failure condition when the flight crew intervenes in control:

- Aircraft impact - if the crew intervenes in control, a significant evolution of the aircraft dynamics, a collision with the g
- Flight crew impact - the flight crew intervenes in the aircraft control, creating a significant control action from the incor

Given the assessment of the failure impact on the aircraft and the flight crew when the crew intervenes in control, the maximum criticality corresponds to CATASTROPHIC (CAT) in connection with the possible occurrence of a significant roll or pitch moment. CAT is classified as a catastrophic situation (prevention of people’s death is almost impossible). Allowable probability (qualitative assessment): almost unbelievable. Allowable probability (quantitative assessment): ≤10-9.

The sidestick move from autopilot signals function FHA shows that its failure cases (in the worst case) leads to CAT situation. It follows that the Functional Development Assurance Level (FDAL) of this function is level “A”, which requires some independence in the design processes (validation, development, verification).

3.1.2 Failure Tree Analysis for “Erroneous active sidestick tracking signals from AFCS” failure case

In order to formulate safety requirements for the The sidestick move from autopilot signals function within the framework of this article, will assume that only a failure case (FC) leading to a CAT will be considered. For this FC, Failure Tree Analysis (FTA) should be carried out in order to determine the requirements budget according to the items development assurance level (IDAL) (transition from FDAL to IDAL) and a quantitative assessment of safety.

The main distinguishing feature of the FTA is the failure analysis taking into account the architecture of the system (implemented or assumed), methods for monitoring failures and implementation in software, firmware and hardware.

To achieve this goal, the FTA will also make some assumptions regarding Sidestick move from Autopilot signals function:

- The control signal for moving the sidestick is generated in AFCS electronics;
- Sidestick as a system has an electronic control unit (sidestick electronics) that converts control signals from AFCS electronics into a moving sidestick actuator;
- Sidestick electronics has its own monitoring system that determines some types of sidestick failures, including runaways;
- AFCS electronics has information about sidestick failures, both through monitoring in sidestick electronics, and based on its own monitoring function.

Functional interaction of AFCS electronics and sidestick system is presented on fig. 4.

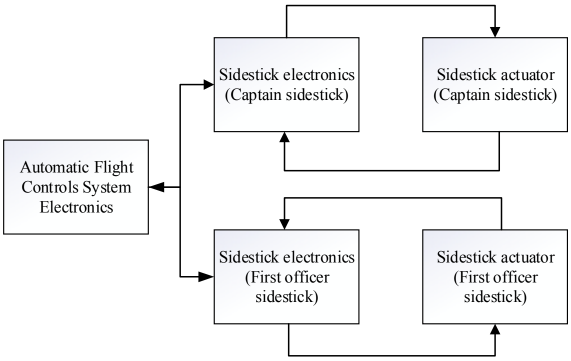

Fig. 4. Functional interface between AFCS electronics and Sidestick system

Subject to the above assumptions and functional diagram, an FTA is possible. FTA is presented in the Fig. 5-7.

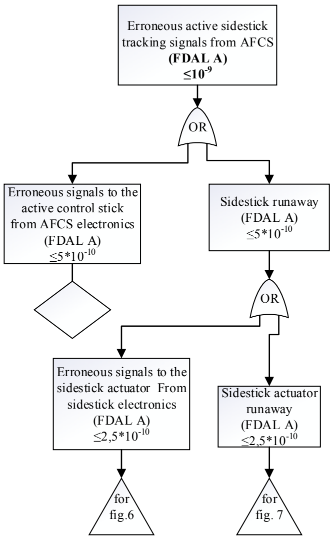

Fig. 5 FTA for FC “Erroneous active sidestick tracking signals from AFCS” (part 1/3)

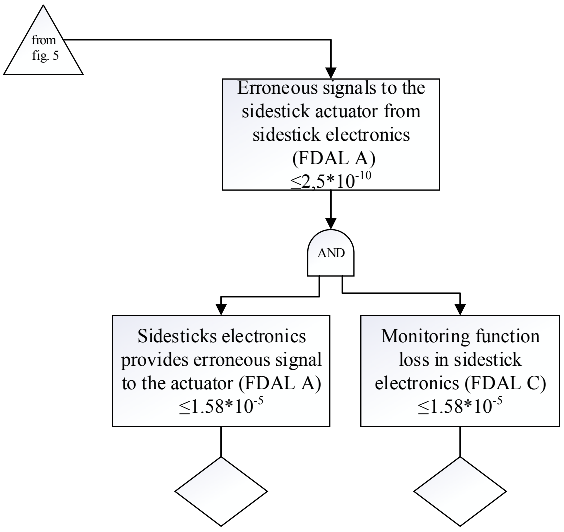

Fig. 6. FTA for FC “Erroneous active sidestick tracking signals from AFCS” (part 2/3)

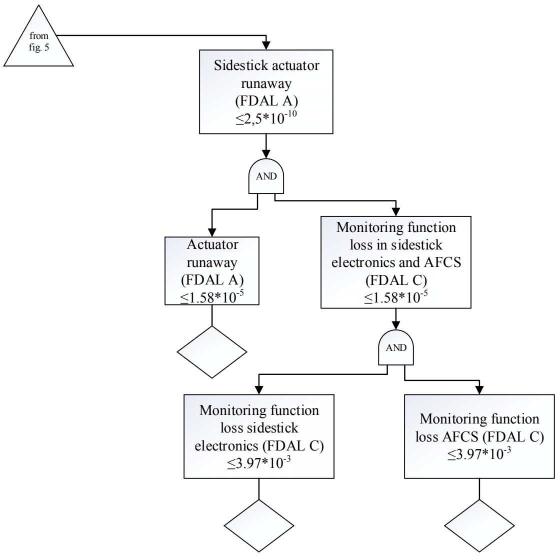

Fig. 7. FTA for FC “Erroneous active sidestick tracking signals from AFCS” (part 3/3)

3.1.3 Common Mode Analysis for “Erroneous active sidestick tracking signals from AFCS” failure case

Recommendations for the Common Mode Analysis [10] distinguish two main steps of the analysis at the stage of preliminary safety assessment:

- Determining the list of potential sources of a common mode of failure;
- Determining safety requirements of independence for each source of the common mode of failure.

A list of potential sources of a common mode of failure is presented in [10]. To determine the requirements for these sources of the common mode of failure, each AND-event of a catastrophic FTA must be identified. From this list of identified combinations, those that are guaranteed to be independent should be selected.

The applicable assumption for the analysis for the sidestick move from autopilot signals function at the current stage of development is the exclusion from the requirements determining in the sections manufacturing, Installation / integration and test, operation, maintenance, calibration and environmental. Thus, at the current stage, the requirements for the concept and design section are determinate.

Table 1 provides a list of failure combinations identified in the FTA for “Erroneous active sidestick tracking signals from AFCS” failure case. This table also defines those combinations that should be guaranteed to be considered in the Common Mode Analysis.

Table 1. Fault Tree AND-Event List

AND-gate	The need for independence
Erroneous signals to the active control stick from AFCS electronics	It is required to ensure independence at the AFCS electronics development level
Sidesticks electronics provides erroneous signal to the actuator AND Monitoring function loss in sidestick electronics	It is required to ensure independence at the sidestick electronics development level
Sidestick actuator runaway AND Monitoring function loss sidestick electronics AND Monitoring function loss AFCS	It is required to ensure independence at the system level between the sidestick and AFCS electronics

From Table 1, it can be seen that at the system level, a Common Mode Analysis should be carried out to ensure the independence of the sidestick and AFCS electronics failures. The following are the necessary requirements to ensure the independence of these failures in accordance with the checklist [10].

For "Concept and design" common mode type, the following common mode sub-types are highlighted:

- Design architecture; Here are the following sources of common modes of failure:
  - Common external sources (ventilation, electrical power);
  - Equipment protections;
  - Operating characteristics (normally running, standby);
- Technology, materials, equipment type; Here are the following sources of common modes of failure:
  - New/Sensible technology;
  - Component type (size, material);
  - Common Software;
  - Component Use;
  - Internal Conditions (temperature or pressure ranges);
  - Initial Condition;
- Specifications; Here are the following sources of common modes of failure:
  - Specification Origin;
  - Same Specification.

Based on the indicated sources of common modes of failures, qualitative safety requirements are determinate. They are presented in section 3.1.4 of this article.

3.1.4 Preliminary Safety Requirements for the sidestick move from autopilot signals function

FTA for FC “Erroneous active sidestick tracking signals from AFCS” allows to formulate the quantitative safety requirements for the sidestick move from autopilot signals function presented in Table 2.

Table 2. Quantitative safety requirements for the sidestick move from autopilot signals function

Item	Requirement
AFCS electronics	FC “Erroneous signals to the active control stick from AFCS electronics” must have a probability of an hour of flight $\leq 5*10^{-10;}$
AFCS monitoring function	FC “Monitoring function loss AFCS” must have a probability of an hour of flight $\leq 3.97*10^{-3}$
Sidestick electronics	FC “Sidesticks electronics provides erroneous signal to the actuator” must have a probability of an hour of flight $\leq 1.58*10^{-5}$
Sidestick monitoring function	FC “Monitoring function loss sidestick electronics” must have a probability of an hour of flight $\leq 1.58*10^{-5}$
Sidestick actuator	FC “Actuator runaway” must have a probability of an hour of flight $\leq 1.58*10^{-5}$

FTA and Common Mode Analysis for FC “Erroneous active sidestick tracking signals from AFCS” allows to formulate the qualitative safety requirements for the sidestick move from autopilot signals function:

- The AFCS electronics should be designed according to the IDAL “A”;
- The AFCS monitoring function should be designed according to the FDAL “C”;
- Sidesticks electronics should be designed according to the IDAL “A”;
- The sidestick monitoring function should be designed according to the FDAL “C”;
- The sidestick actuator should be designed according to the IDAL “A”;
- In case of using ventilation for the sidestick and AFCS electronics, the ventilation sources must be independent OR it must be proved that the loss of ventilation of both components cannot lead to both situations: Sidestick runaway AND Monitoring function loss AFCS;
- The power supplies for the sidestick and AFCS electronics must be independent OR it must be proven that the power loss (or erroeneous power supply) of both

components cannot lead to both situations: Sidestick runaway AND Monitoring function loss AFCS;
- Operating characteristics (normally running, standby) cannot be a source of a common cause of failure, because both functions (control and monitoring) are carried out simultaneously throughout the flight;
- Active sidestick is a new technology. Development should be carried out taking into account the requirements of [6, 7, 8, 9, 10] to minimize the risk of unintended dysfunctions;
- Sidestick and AFCS electronics Hardware should be developed according to DAL A and C respectively. In this case, developers must be independent;
- Sidestick and AFCS electronics Software should be developed according to DAL A and C respectively. In this case, developers must be independent;
- Sidestick and AFCS electronics should not have the same components in their architecture OR it must be proven that any possible failures of this component cannot lead to both situations: Sidestick runaway AND Monitoring function loss AFCS;
- AFCS electronics ventilation should be used if operation in excess of the expected temperature may result in Monitoring function loss AFCS;
- Sidestick ventilation should be used if operation in excess of the expected temperature may result in Monitoring function loss AFCS;
- Initial Condition cannot be a source of a common cause of failure, as both functions (control and control) are carried out simultaneously throughout the flight.

Depending on specific architectures, requirements may vary and be specified.

4 Conclusion

Currently, there is a tendency in the world to move from controlling civilian aircraft using yokes to controlling using sidesticks. However, with the advent of side sticks, instead of yokes, a problem began to arise due to the lack of tactile feedback to the flight crew about the position of the aircraft. Such problems are associated with this, as indicated in [3]. The authors also identified a problem with automatic approaches to ICAO categories IIIa and IIIb.

The article considers the architectural possibility of introducing active pilot controls by the example of sidesticks, and shows the difference from the classical architectures of FBW and AFCS. The prerequisites for the implementation of these methods to increase flight crew awareness of the spatial position of the aircraft are indicated.

Given that the introduction of a new function on an aircraft entails the need for safety analyzes to ensure the safety assessment process, the potential hazards of the sidestick move from autopilot signals function are evaluated. According to the results of the FHA, it was revealed that the required FDAL for this function is level “A”.

In accordance with the FC, leading to a CAT, a preliminary FTA was carried out. Its result was the requirements for the IDAL participating in the considered function – AFCS electronics, sidestick electronics, sidestick actuator. The FDAL was also determined for monitoring functions of AFCS and sidestick electronics.

Further work on this topic will include tasks such as:

- Validation of derivative safety requirements obtained in the course of the Common Mode Analysis;
- Development and validation of an algorithm for moving active sidesticks by signals from AFCS;
- Verification of this function with the pilot in the control loop to evaluate the requirements of CS 25.671.

It should be noted that active sidesticks are an actual direction in the development of science and technology [13, 14]. The materials of the work done allow to supplement the developments available in the international community with the necessary safety requirements that ensure reliability and flight safety, as well as supporting the certification process of civil aircraft.

Active pilot controls are planned for certification on the MC-21 (Irkut’s Corporation aircraft) [15]. The second session of certification flights of the MC-21 aircraft by EASA ended in June 2019 [16]. The decisions made during the design of FBW regarding the use of active pilot control sidesticks were positively evaluated, including at minimum take-off and landing speeds, as well as simulating a critical engine failure.

Based on the results of bench and flight tests of the MC-21 aircraft, it will be possible to draw a conclusion about the hypotheses put forward in this article, about reducing the time for recognizing failure and taking control of the pilots when performing the autopilot function using active controls.

References:

[1] Li X., Li B., Liu H. Discussion on the Application of Active Side Stick on Civil Aircraft. In: Yamamoto S., Mori H. (eds) Human Interface and the Management of Information. Information in Applications and Services. HIMI 2018. Lecture Notes in Computer Science, vol 10905. Springer, Cham pp. 441 – 449.

[2] Gratton G. (2018) Control Surfaces and Circuits. In: Initial Airworthiness. Springer, Cham pp. 167-189.

[3] Wolfert F., Bromfield M. A., Scott S., Stedmon A. Passive Sidesticks and Hard Landings - Is there a Link? AIAA Aviation 2019 Forum

[4] Bartley G 2001 Boeing B-777: Fly-ByWire Flight Controls The Avionics Handbook ch.11

[5] Hanke D and Herbst C 1999 Active sidestick technology – a means for improving situational awareness Aerospace Science and Tech. vol 3 Issue 8 pp 525–532

[6] Aerospace Recommended Practice ARP4754A. Guidelines for Development of Civil Aircraft and Systems. – The USA: SAE International, 2010. – 115 p.

[7] Software Considerations in Airborne Systems and Equipment Certification DO-178C. –Washington, 2011. – 144 p.

[8] Design Assurance Guidance for Airborne Electronic Hardware DO-254. – The Washington, 2000. – 137 p.

[9] European Aviation Safety Agency 2007 Certification Specifications for Large Aeroplanes CS-25 Amendment 3

[10] SAE ARP 4761 1996 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment SAE International p 311

[11] Wilkinson. P. J., Functional hazard analysis for highly integrated aerospace systems. / T.P. Kelly. // IEE Certification of Ground/Air Systems Seminar. – 1998. – 1998p.

[12] Fussell, J. B., Fault tree analysis: concepts and techniques // Pressure vessels and piping: design and analysis. – New York. – 1976. – № 4. – p. 417-431.

[13] Begin M, Denninger M and Plante J 2019Design and Experimental Validation of a 2DOF Sidestick Powered by Hyper-Redundant Magnetorheological Actuators Providing Active Feedback, 2019 International Conference on Robotics and Automation (ICRA)

[14] Fu W, Van Paassen M, Mulder M, Developing Active Manipulators in Aircraft Flight Control // Journal of Guidance, Control, and Dynamics vol 42 num 8, 2019

[15] Irkut MC-21 Aircraft https://www.aerospace-technology.com/projects/irkut-21-aircraft/ (20.10.2019)

[16] EASA flight test experts completed the second session of certification flights http://eng.irkut.com/press-centre/news/2392/ (17.06.2019)