33RD CONGRESS
OF THE INTERNATIONAL COUNCIL
OF THE AERONAUTICAL SCIENCES
STOCKHOLM, SWEDEN, 4-9 SEPTEMBER, 2022

ICAS 2022 SWEDEN

The New Research Aircraft ISTAR - Experimental Flight Control System

Dominik Niedermeier[1], Kai Giese[2], Dirk Leißling[3]

[1] German Aerospace Center, Institute of Flight Systems, Braunschweig, 38108, Germany
[2] German Aerospace Center, Institute of Flight Guidance, Braunschweig, 38108, Germany
[3] German Aerospace Center, Flight Experiments, Braunschweig, 38108, Germany

Abstract

This paper describes the design of DLR's new research aircraft Falcon 2000LX ISTAR (In-flight Systems & Technology Airborne Research). After having received the modified aircraft in 2020 additional modification phases shall enhance the capabilities of the aircraft for its future application as Variable Stability System (VSS) and for rapid inflight testing of any Guidance, Navigation and Control (GNC) research software application. The most essential modification of the aircraft will be the integration of an Experimental Flight Control System (EFCS) allowing control surface inputs generated by uncertified research flight control hard- and software. To operate the EFCS a specific safety and operational concept is required. New failure conditions introduced by the integration of the EFCS have been defined to perform a Functional Hazard Analysis (FHA) leading to functional safety requirements, such as reliabilities and Functional Design Assurance Levels (FDAL), for each function. For the criticality assessment of certain failure condition pilot-in-the-loop simulations have been performed in the Air Vehicle Simulator (AVES). Based on the performance and safety requirements a preliminary EFCS design has been defined.

Keywords: Variable Stability System, Experimental Flight Control System, Functional Hazard Analysis

1. Nomenclature

AFCS	=	Automatic Flight Control System
AVES	=	Air Vehicle Simulator
BASIC	=	Basic Mode
BASIC EXP	=	Basic Experimental Mode
CoA	=	Certificate of Airworthiness
DLR	=	German Aerospace Center
EASA	=	European Union Aviation Safety Agency
EFCS	=	Experimental Flight Control System
EGP	=	Experimental Guidance Panel
EP	=	Experimental Pilot (right-hand seat)
FBW	=	Fly-by-Wire / Fly-by-Wire Mode
FBWCL	=	Fly-by-Wire Command Limiter
FBWCP	=	Fly-by-Wire Command Protection
FBWS	=	Fly-by-Wire System
FDAL	=	Functional Design Assurance Level
FHA	=	Functional Hazard Assessment

FL	=	Flight Level
GNC	=	Guidance, Navigation & Control
HS	=	Horizontal Stabilizer
ISTAR	=	In-flight Systems and Technology Airborne Research
LH	=	left-hand
MCP	=	Mode Control Panel
PDU	=	Primary Display Unit
RCS	=	Research Computer System
RES	=	Research Mode
RH	=	right-hand
SP	=	Safety Pilot (left-hand seat)
TCU	=	Throttle Control Unit

2. Introduction

In 2020 the German Aerospace Center (DLR) received its new research aircraft ISTAR (In-flight Systems and Technology Airborne Research) based on a modified Dassault Falcon 2000 LX (see Figure 1). After having signed the purchase contract in 2018 the former Dassault prototype which was used for avionics certification was refurbished in order to receive a Certificate of Airworthiness (CoA) from the European Aviation Safety Agency (EASA). The ISTAR project currently foresees three different project phases. Each project phase includes a modification phase and a research application phase. The objective is the integration of an Experimental Flight Control System (EFCS) with access to all primary and secondary control surfaces which allows ISTAR to be used as a Variable Stability System (VSS), e.g. for test pilot school applications, or for any Guidance, Navigation and Control (GNC) research application. The EFCS shall allow the rapid integration and flight testing of GNC software code without having to rely on a time-consuming software approval process.

A joint design team, composed of Dassault and DLR experts, has worked on the EFCS architecture with the main focus on the capability to send commands generated by the research GNC software to the existing autopilot aileron and elevator servomotors as well as to a new servomotor used for rudder control. For experimental thrust control the existing autothrottle motor integrated in the Throttle Control Unit (TCU) provides an interface to the research software. Finally, an experimental access to the Horizontal Stabilizer (HS) allows automatic trim to be performed by the EFCS.

One of the main design drivers for the design of the EFCS is the safety concept that relies mainly on the safe and reliable reversion to the basic mechanical flight control system in any flight condition.

Figure 1 – The new DLR research aircraft ISTAR

3. ISTAR Project Phases

In 2018 DLR purchased a Dassault Falcon 2000LX prototype with the serial number S/N 006, which served for the certification of the Honeywell EASy II cockpit and for the winglet modification. Before being delivered the aircraft was refurbished in order to obtain a Certificate of Airworthiness.

As part of this modification the experimental power supply by an additional third generator was implemented. Several experimental antennas were added. For structural health monitoring research, the aircraft was equipped with accelerometers and strain gauges distributed over the wings, the fuselage and the empennage as well as the engine inlets. The nose cone can be exchanged such that a nose boom for undisturbed air data measurements can be installed (see Figure 2). A new data acquisition system was integrated in order to acquire data from the aircraft data busses, the nose boom and additional experimental sensors, such as an inertial platform as well as the accelerometers and the strain gauges (see Figure 2).

In addition to that, in preparation for future research applications a specific cabin layout including provisions for the integration of a flight test engineer station, the data acquisition system and additional racks was specifically certified for the F2000LX S/N 006.

It is planned to integrate a datalink allowing the operation of a telemetry station and an uplink enabling control of the aircraft from ground for unmanned system research applications.

Currently first flight tests are performed that aim at validating DLR’s aerodynamic computation tools and improving the already available flight dynamics model of the ISTAR. This flight dynamics model will be used for desktop and pilot-in-the-loop simulations required for the definition of the performance and safety requirements during the design phase. In a second step the model will be used for the design of the experimental autopilot and autothrottle controllers as well as of the EFCS.

The ISTAR project is divided into different modification phases. Each phase includes engineering work, the corresponding modification of the aircraft and a time span in which the aircraft is used for research applications. Based on the planned research applications the final task of all aircraft modifications is the capability to perform efficient flight testing of uncertified GNC software applications by integrating an EFCS.

3.1 Research Applications

The planned research applications drive the top-level requirements, which define the necessary modifications of the basic Dassault F2000LX aircraft.

The following research applications are planned on the testbed:

In-flight Simulation

- Handling qualities evaluation for new aircraft configurations
- Variable stability, e.g. for test pilot school training
- Simulation of atmospheric disturbance, e.g. wake vortex encounter

General Flight Control Applications

- Maneuver- and Gust-Load Alleviation
- System identification of aero-elastic properties
- Formation flight
- Air-to-air refueling

Flight Guidance

- Future approach procedures
- 4D-Navigation
- Low-level flight guidance
- New autopilot functions
- Automatic taxiing
- Remotely Piloted Air System surrogate

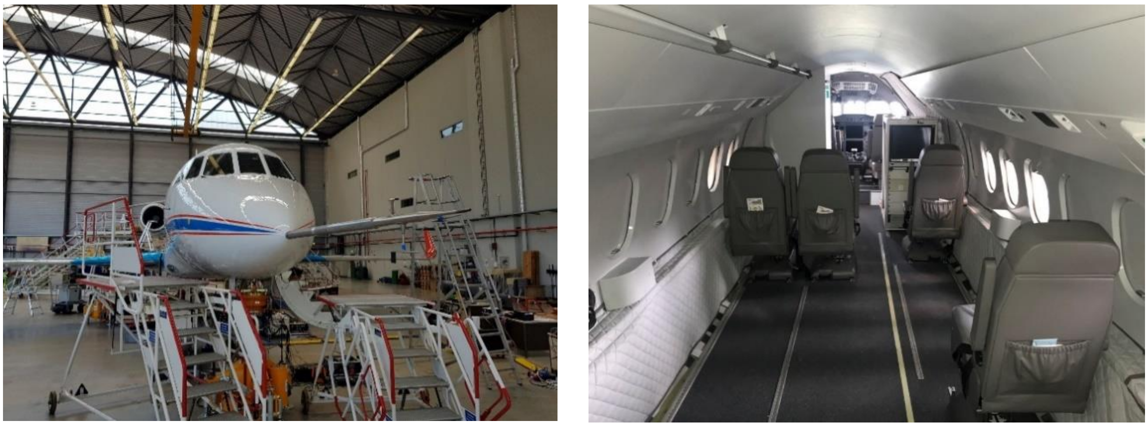

Figure 2 – ISTAR nose boom installation and cabin layout incl. data acquisition system

3.2 Implementation of the EFCS

The EFCS comprises all system components that are required to perform flight testing of GNC software applications. In the first step the following EFCS capabilities will be realized:

- Experimental access to the existing aileron and elevator autopilot servomotors
- Integration of a new rudder servomotor providing experimental access to the basic mechanical rudder control
- Experimental access to the existing horizontal stabilizer motor
- Experimental access to the existing autothrottle motor
- Integration of an experimental display in front of the basic aircraft displays on the right-hand side of the cockpit

The initial modifications will allow the Experimental Pilot (EP) seated on the right-hand side to provide command inputs for the research flight control software via an Experimental Guidance Panel (EGP). In a next step manual control inputs to the EFCS will be realized by integrating experimental control inceptors, such as an experimental sidestick and pedals, on the right-hand cockpit side allowing testing of manual control laws and variable stability for test pilot training.

The control surface commands provided by the EFCS are generated by uncertified software applications. These software applications and their corresponding hardware shall not comply with any safety requirement as their main task is to allow a rapid integration of research software. These system components are grouped in the so-called Experimental System.

Note that the Experimental System is considered as the unreliable part of the EFCS. The probability that the Experimental System computes unintended commands, such as hardover commands, is assumed to be equal to 1 during the safety assessment process.

Additional system components will be required to guarantee safe operation of the ISTAR. These safety-relevant components have to comply with safety requirements derived from an FHA. The most important safety-relevant system component performs the reliable and safe disconnect of the EFCS from the basic mechanical flight control system in any flight condition. These EFCS components are not part of the Experimental System.

4. General Safety Concept

According to the requirements defined in Section 3 the main task of ISTAR is to allow a rapid integration of uncertified research software applications without requiring a costly software certification process.

However, one important step is the integration and the testing of the software into the newly developed ISTAR ground based simulator. After the software has been tested and cleared by the crew it is integrated into the ISTAR. A new research flight control software shall be ready for flight within a few days. But as there is no required software development process, systematic errors in the implementation of the research software are likely to occur. This has to be accounted for in the definition of the Safety Concept and in the design of the EFCS architecture as well as in the FHA (see Section 7).

The probability for the loss of Experimental System functions or unintended commands that are computed within the Experimental System is considered to be equal to 1. This will be further elaborated in Section 7. This assumption forms the basis for the entire safety concept on which the operation of the ISTAR is based.

The safety of the aircraft is guaranteed by the highly reliable switching from the EFCS to the basic mechanical flight control system. The safety concept relies on the ability of the Safety Pilot to make correct judgements regarding unsafe experimental control inputs or flight conditions or developing risks and hazards before these become immanent and compromise flight safety. The switching has to be instantaneous and transient free [1].

For that reason, the criticality of particular failure events arising from the EFCS is strongly dependent on the reaction time of the Safety Pilot. In case of events or flight phases in which the reaction time of the Safety Pilot is not sufficient to guarantee safe operation of the ISTAR the reliable disconnect function is not sufficient either and additional safety functions are required.

4.1 Safety Pilot Monitoring Cues

The Safety Pilot is supported by different cues that enable to detect an unsafe situation and to switch to the basic mechanical control system as fast and as reliable as possible.

Safety Pilot Cues to Monitor Experimental Control System Commands

The control wheel, the control column and the pedals of the Safety Pilot as well as the power levers are moved in correspondence with the control surface deflections and the thrust commanded by the EFCS. The movement of the control inceptors and the throttle levers is an important cue for the Safety Pilot to anticipate the aircraft to enter an unsafe flight condition already based on the control inputs.

Safety Pilot Cues to Monitor Relevant Flight Parameters and Control Forces

As the whole safety concept relies on the Safety Pilot's ability to detect unsafe EFCS commands or flight conditions as quickly as possible, a reliable indication of the relevant flight control and flight condition parameters is essential. Most relevant flight parameters are presented on the basic aircraft Primary Display Unit (PDU). However, other parameters that are essential are presented on a dedicated additional display on the left-hand side of the cockpit. A very important indication is the elevator, aileron and rudder force display which is fed with the servomotor currents. It provides information on the forces that the Safety Pilot has to exert after the EFCS has been disconnected. The active mode and all mode changes related to the EFCS modes are also presented on this display.

Aural Warning and Cautions

Every mode change related to the EFCS modes (see Section 5.1) is indicated by a sound. In case of a disconnect an aural warning is triggered.

4.2 Pilot Reaction Time

To keep the system complexity as low as possible protection and monitoring functions shall be only applied, if the Safety Pilot's reaction time is not sufficient to prevent a hazardous or even catastrophic event. This is especially important when ISTAR is operated close to the ground, where the available reaction time is very limited due to a pending uncontrolled ground impact or at high speeds where structural damages can occur before the Safety Pilot is able to disconnect. For that reason, the pilot reaction time has a direct impact on the system design and on the operational envelope of the EFCS.

As a reasonable assumption for the Safety Pilot reaction time of 1 s was chosen for the severity classification as part of the FHA and for the resulting system design. This assumption was derived from [2].

4.3 Manual Disconnect

By depressing disconnect buttons on the yoke and on the TCU the Safety Pilot is able to revert back to the basic mechanical flight control at any time. As disconnect buttons the basic autopilot and autothrottle disconnect buttons will be used.

In addition, by exceeding a certain force threshold on the yoke or the pedals the Safety Pilot is able to revert back to the mechanical flight control at any time. The forces required to override the Experimental System and initiate its disengagement while reengaging the basic system shall be high enough to avoid an inadvertent deactivation of the Experimental System. On the other hand, the forces shall not induce an over control situation of the aircraft following the deactivation of the Experimental System.

4.4 Authority Limitation and Automatic Disconnect

Generally, two different approaches for additional safety functions can be distinguished, if the Safety Pilot reaction time is not sufficient:

- Provide the Safety Pilot with at least 1 s to take over before a hazardous or catastrophic event occurs by limiting the authority of the system in a reliable way
- Automatically disconnect the Experimental System, if servomotor malfunctions that lead to hazardous or catastrophic event are detected.

5. Operational Concept

The operational concept of the ISTAR describes the operating modes of the aircraft and the tasks of the flight crew. It is based on the flight control research application and safety concept requirements.

5.1 Operating Modes

According to the operational concept of the ISTAR the aircraft shall be operated in four different modes that are usually activated and de-activated in sequence as long as a quick disconnect of the EFCS is not necessary (see Figure 3). Depending on the research application the Experimental Display is available on the right-hand side of the cockpit in all modes (BASIC, BASIC EXP, FBW and RES).

Basic Mode (BASIC)

The primary control surfaces are controlled via the basic mechanical flight control system using control wheel, control column and the rudder pedals (Safety Pilot station). The control of the flaps/slats, airbrakes and throttles corresponds to the controls of the basic aircraft. In the Basic Mode, the basic autopilot and autothrottle functions are completely functional. All EFCS components are switched off and completely passive.

Basic Experimental Mode (BASIC EXP)

The primary control surfaces are controlled via the basic mechanical flight control system using control wheel, control column and the rudder pedals (Safety Pilot station). The control of the flaps/slats, airbrakes and throttles corresponds to the controls of the basic aircraft. In the Basic Experimental Mode, the basic autopilot and autothrottle functions are completely functional. All parts of the EFCS including the data acquisition system are powered (FBW_PWR_ON). In this mode the integrity and connection checks are performed to arm the Fly-by-Wire Mode. The commands generated by the Experimental System are not sent to the servomotors.

Fly-by-Wire Mode (FBW)

The FBW Mode allows control of the aircraft from the right-hand pilot seat (Experimental Pilot). The pilot commands are sent from the experimental control inceptors or the EGP to the Experimental System which generates the commands for the servomotors. The FBW Mode hosts default control laws and the default experimental autopilot. It will be used to stabilize the aircraft or to establish a new test point before the RES mode is activated. The Experimental Display is active and its contents may be switched by the Experimental Pilot.

Research Mode (RES)

The RES Mode allows control of the aircraft from the right-hand pilot seat (Experimental Pilot). In contrast to the FBW Mode the control surface commands are computed by a software application that is specific to every flight experiment. The RES Mode hosts a framework that allows the rapid integration of Matlab/Simulink® models via the Real-Time Workshop® or the Simulink Coder®. Depending on the experiment the software application might generate directly control surface commands or setpoints for the default experimental autopilot hosted by the FBW Mode. The Experimental Display is active and its contents may be switched by the Experimental Pilot.

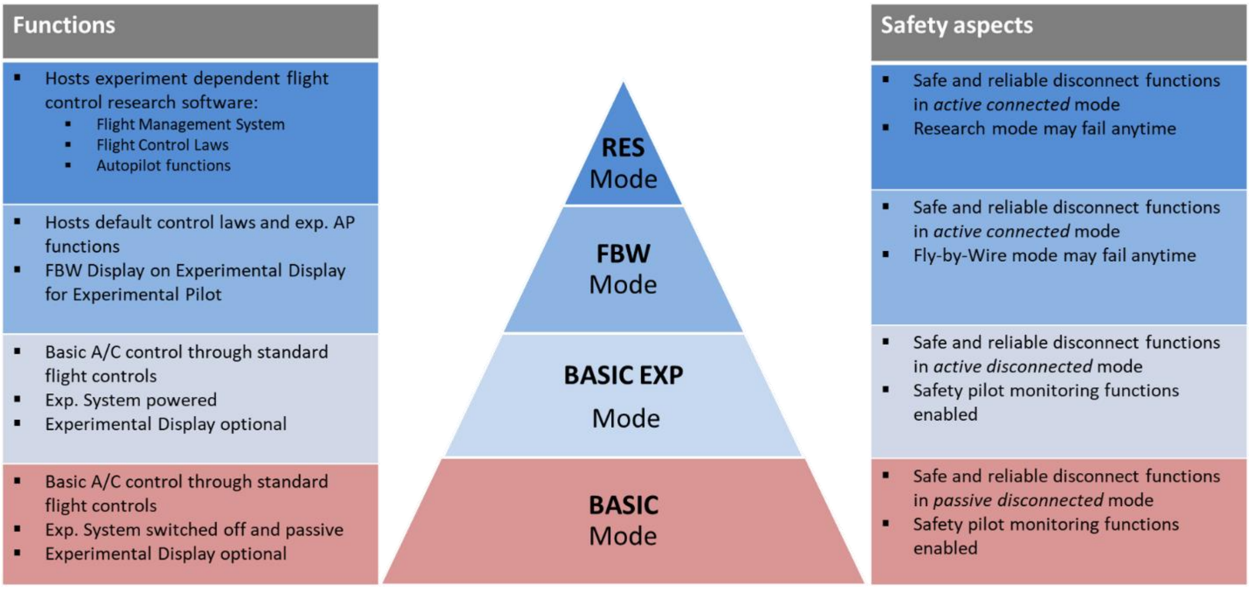
Functions
Hosts experiment dependent flight control research software:
Flight Management System
Flight Control Laws
Autopilot functions
Hosts default control laws and exp. AP functions
FBW Display on Experimental Display for Experimental Pilot
Basic A/C control through standard flight controls
Exp. System powered
Experimental Display optional
Basic A/C control through standard flight controls
Exp. System switched off and passive
Experimental Display optional
RES Mode
FBW Mode
BASIC EXP Mode
BASIC Mode
Safety aspects
Safe and reliable disconnect functions in active connected mode
Research mode may fail anytime
Safe and reliable disconnect functions in active connected mode
Fly-by-Wire mode may fail anytime
Safe and reliable disconnect functions in active disconnected mode
Safety pilot monitoring functions enabled
Safe and reliable disconnect functions in passive disconnected mode
Safety pilot monitoring functions enabled

Figure 3 – ISTAR Operating Modes

5.2 Mode Switching

The transitions between the operating modes are controlled by the flight crew using a dedicated panel designated as Mode Control Panel (MCP). The MCP ensures that the preconditions for a change of the operating mode are fulfilled in each case. By engaging the BASIC Experimental Mode, the power supply of all EFCS components is activated. The BASIC EXP Mode contains two submodes: FBW OFF and FBW ARMED. The FBW OFF Mode is always invoked after the engagement of the BASIC EXP Mode. To operate the aircraft in FBW Mode, the crew must first arm the Experimental System via the MCP, so that necessary checks can be performed after reaching FBW ARMED Mode. When all requirements are met, the crew can switch to the FBW Mode. In FBW Mode the crew can engage the RES Mode by pressing the corresponding button on the MCP (see Figure 4).

The deactivation of the FBW Mode can be triggered via the MCP or at any time by a quick disconnect that instantaneously switches back to the BASIC Mode allowing immediate control of the aircraft via the basic mechanical flight control system.

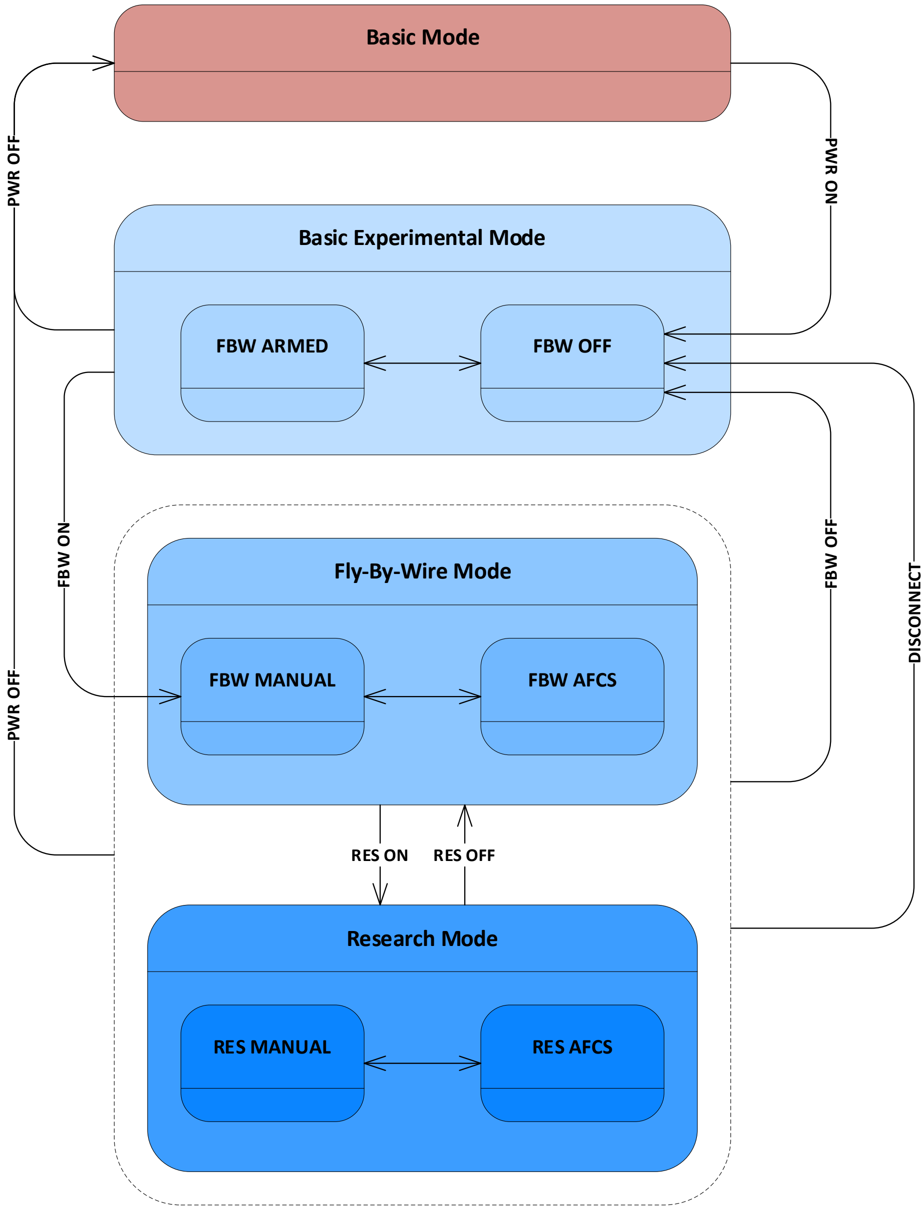

Figure 4 – ISTAR Mode Switching

5.3 Roles of the Crew Members

The crew is composed of the Safety Pilot, the Experimental Pilot, the Flight Test Engineer and the Experimenter.

Safety Pilot (SP)

The Safety Pilot sits in the left-hand seat and is pilot in command (PIC). With the aircraft in BASIC and BASIC EXP Mode and regardless of his duties as PIC he has access to the basic flight control system and can act either as Pilot Flying or Pilot Monitoring.

With the aircraft in FBW or RES Mode he acts as Pilot Monitoring and closely monitors the flight condition of the aircraft considering the course of the preceding flight. If he detects an unsafe flight condition or if he anticipates the aircraft to enter an unsafe flight condition he takes over control either by manual disconnection or by means of force override. In any case it is his responsibility to ensure the safety of the flight any time.

Experimental Pilot (EP)

The Experimental Pilot is Co-Pilot and sits in the right-hand seat. In BASIC and BASIC EXP Mode the EP can act as Pilot Flying or as Pilot Monitoring. In FBW- or RES-Mode the EP is always Pilot Flying. The Experimental Pilot activates the FBW- or RES Mode on command of the Safety Pilot.

In case of any uncontrollable behavior of the aircraft the Evaluation Pilot hands over control back to the Safety Pilot. The EP conducts the experimental flight task according to instructions of the researchers. He answers the queries of the researchers who designed the experiment and provides pilot ratings.

Flight Test Engineer

The Flight Test Engineer is part of the crew and sits at the FTE-Station in the cabin. He guides the course of the flight test and monitors relevant flight parameters. He informs the flight crew if he detects any kind of undesired aircraft or system behavior.

Experimenter

The Experimenter is an optional crew member. One or more Experimenters may be on board of a flight if required by scientific reasons in order to e.g.

- observe the flight test and in-situ judge flight test results.
- assist the FTE in conducting the Flight Test.
- operate scientific equipment.

6. Experimental Flight Control System (EFCS) Design

6.1 General Concept

The concept for the EFCS architecture has been worked out during an extensive common design process performed by Dassault Aerospace and DLR that resulted in the identification of overall safety requirements. With respect to the later technical implementation of required functions, associated system responsibilities were defined and corresponding interface requirements have been derived. Figure 6 presents the system design of the EFCS.

6.2 High-Level System Architecture

The following section describes the main systems of the Experimental Flight Control System as defined in the ISTAR High-Level Technical Requirements [3].

Fly-by-Wire System

The Fly-by-Wire System represents the key element of the Experimental System. This system will basically provide the following functions:

- Input/output interfacing to basic aircraft systems
- Data consolidation and integrity testing
- Communication functions with different subsystems and peripheral devices
- System monitoring and failure detection
- Task control, application management and software flow control
- Default fly-by-wire functions for automatic and manual flight control

command monitoring and limitation (in terms of certification not reliable)

Among the pure system functions it will be the main task of the Fly-by-Wire System to compute the nominal control surface and power lever deflection commands and send it to the servomotors. In the first instance, it will exclusively be possible to generate these commands using the default experimental automatic and manual flight control functions in combination with the Experimental

Guidance Panel (EGP) as cockpit input device.

The Mode Control Panel (MCP)

The MCP is the pilots' interface to select the different modes and functions of the EFCS as described in Section 5. In addition, the MCP is used to activate the FBWCL and FBWCP functions when the aircraft approaches a certain altitude above ground level or when certain airspeed threshold is exceeded.

Research Computer System (RCS)

The Research Computer System executes the research applications. The output of these applications primarily consists either of desired control surface deflection commands or predetermined desired values for the experimental autopilot, autothrottle, and autotrim applications (e.g. selected airspeed, altitude, heading, Mach number, etc.). The system does not have a direct link to the control interfaces of the servomotors and interacts with the Fly-by-Wire System.

Fly-by-Wire Command Limiter (FBWCL)

In contrast to the internal command limiting function of the Fly-by-Wire System the FBWCL will be a part of the safety-relevant systems. Under flight conditions near to the ground it shall guarantee a safe takeover by the Safety Pilot within a predefined reaction time, at high speed it shall prevent the aircraft, especially the vertical stabilizer, from structural damage. These functions are achieved by limiting the control surface deflection commands in terms of rate and position. The FBWCL is activated manually by the flight crew using the MCP.

Fly-by-Wire Command Protection (FBWCP)

The FBWCP shall automatically initiate a disconnection of the experimental system in the case of an identified primary control servomotor failure or if the pre-defined rate and deflection limits are exceeded. The FBWCP is activated by the flight crew using the MCP.

The Servomotor Interface and Disconnection System (SIDS)

The Servomotor Interface and Disconnection system will ensure an exclusive, safe, and reliable switching of the connections between the basic aircraft's autopilot, autothrust and autotrim HS command output on the one hand and the corresponding command outputs of the EFCS on the other hand to the servomotors and horizontal stabilizer trim actuator.

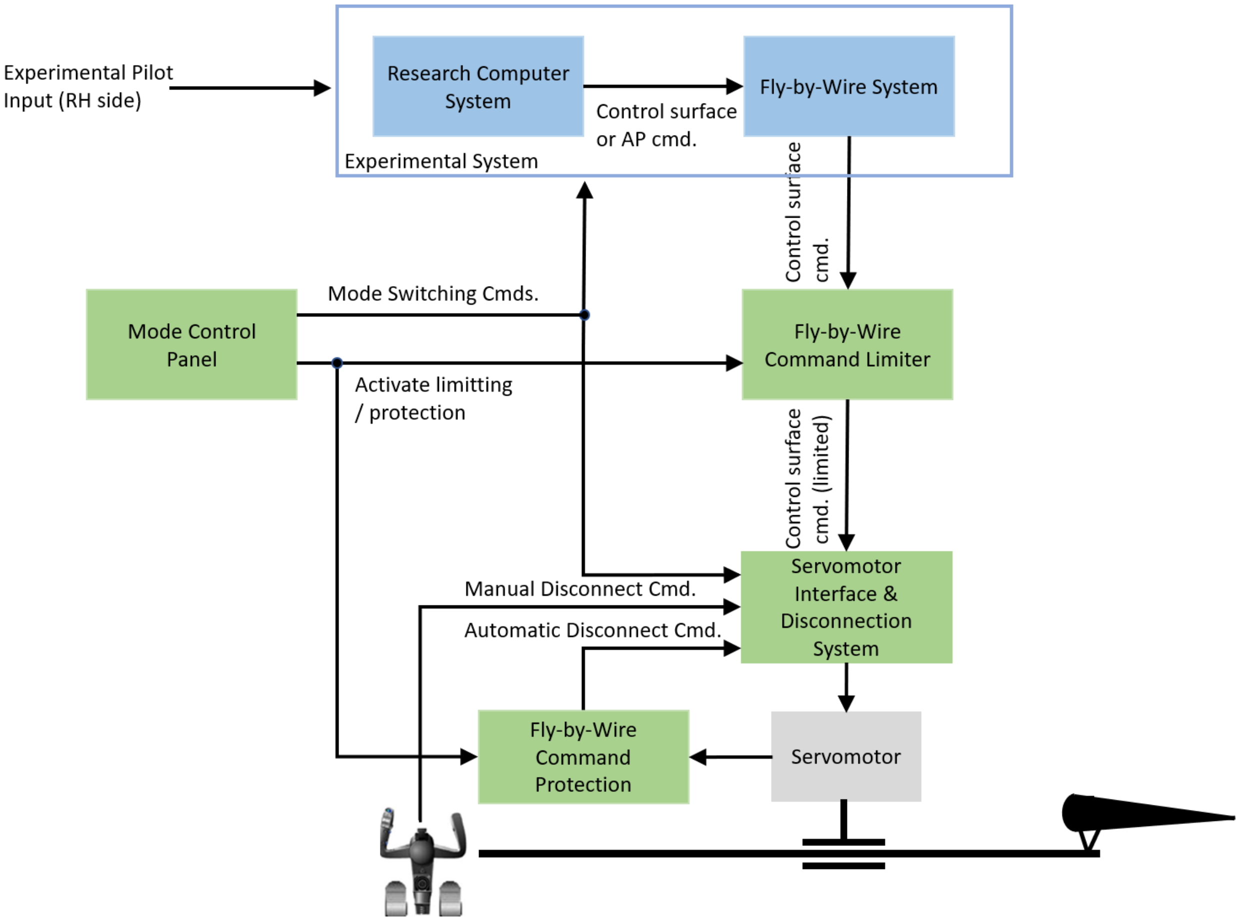
Experimental Pilot
Input (RH side)
Research Computer System
Fly-by-Wire System
Control surface or AP cmd.
Experimental System
Control surface cmd.
Mode Switching Cmds.
Mode Control Panel
Fly-by-Wire Command Limiter
Activate limitting / protection
Control surface cmd. (limited)
Manual Disconnect Cmd.
Automatic Disconnect Cmd.
Servomotor Interface & Disconnection System
Fly-by-Wire Command Protection
Servomotor

Figure 5 – EFCS system design (primary axes)
(green = safety-relevant, blue = experimental/research, grey = basic aircraft component)

7. Functional Hazard Assessment

As part of the design process a Functional Hazard Assessment (FHA) was performed [4]. This section outlines some of the main results of the FHA with the focus on failures arising from the EFCS.

It has to be noted that the probability for unintended commands generated by the Experimental System being the unreliable part of the EFCS is considered to be equal to 1. Unintended commands include hardover commands and oscillations including doublets.

7.1 Unintended Commands Generated by the Experimental System

As described in Section 4 an unintended command provided by the Experimental System might always occur. The general safety concept is that the Safety Pilot takes over and recovers the aircraft before hazardous flight conditions are reached. Considering the dynamics of the aileron and elevator servomotor and the pilot reaction time this is the case for all flight conditions above 500 ft AGL. In these cases, a specific limitation of the Experimental System commands is not needed, because the Safety Pilot reaction time is sufficient to prevent hazardous or even catastrophic incidents.

During descent a dedicated function designated the FBWCL function (see Section 6) is activated manually by the crew below 500 ft AGL. This function limits Experimental System commands in terms of deflection rate and deflection angle in order to prevent the aircraft from touching the ground before the Safety Pilot is able to take over which would then result in a catastrophic accident. This limitation is applied to all three primary control axes.

The overall task of the FBWCL is to provide the Safety Pilot with sufficient time to enable him to manually disconnect the EFCS. The values for the FBWCL rate and deflection limits are first determined pilot-in-the-loop simulation and then in real flight testing after the ISTAR with integrated EFCS is available.

7.2 Unintended Commands Resulting from Servomotor Malfunction

An unintended command to the flight control surfaces might also occur in case of a servomotor malfunction. In this case the FBWCL would not prevent a hazardous or catastrophic event when the aircraft is close to the ground. To meet the safety requirements for this failure condition an additional function that monitors the servomotor rates and deflections is necessary. This mitigation function is designated as Fly-by-Wire Command Protection (FBWCP). The FBWCP monitors the servomotor deflections as well as its deflection rates. If an unintended command reaches the pre-defined deflection angle or deflection rate thresholds, the servomotors will be automatically disconnected from the basic mechanical flight control system and the Safety Pilot will regain control of the aircraft. This results in an automatic mode transition from FBW or RES to BASIC EXP Mode. This function is applied to all three primary control axes, too. The values for the FBCWP rate and deflection thresholds correspond to those of the FBWCL. The FBWCP is manually activated by the same signal as the FBWCL.

7.3 Unintended Commands with Loss of all Mitigation Functions Close to the Ground

As described in the preceding sections two mitigation functions take care of unintended commands generated either by Experimental System or by a servomotor malfunction: The FBWCL and the FBWCP functions. If both mitigations are lost close to the ground and a hardover command occurs on one of the primary control axes, the Safety Pilot will not be able to take over control in time and an uncontrolled ground contact might lead to a catastrophic event.

Hence the loss of both functions, FBWCP and FBWCL, shall be extremely improbable according to the certification regulations. As both functions are completely independent from each other, the required overall reliability and corresponding FDAL are allocated to both functions.

As both independent functions, FBWCP and FBWCL, have to fail before the catastrophic event occurs, each function has to be developed according to DAL B [4]. Assuming that the probability of occurrence for a loss of both functions shall be less than 10^{-9}, for each function a safety objective of 10^{-5} would comply with the requirement resulting from this failure condition.

7.4 Unintended Rudder Command with Loss of all Mitigation Functions at High Speed

Considering the authority of the additional rudder servomotor an unintended rudder command, for instance a doublet, might cause structural issues at the vertical tail plane above a certain calibrated airspeed threshold. As these unintended rudder commands are hard to detect by the Safety Pilot, the pilot reaction time might not be sufficient to disconnect the servomotors from the basic mechanical flight control before a structural damage occurs.

For that reason, the FBWCP and FBWCL are not only used below a certain altitude above ground level but also above the speed threshold at which a structural damage at the vertical tail plane might occur in case of a commanded full-deflection rudder doublet.

As a structural vertical tail plane failure will result in a catastrophic event this failure condition results in the same safety objective requirements for the FBWCP and FBWCL functions as for the failure condition described in Section 7.3.

7.5 Loss of Disconnect Function

This failure condition describes a complete loss of the disconnect function. In this case the Safety Pilot is not able to disconnect the EFSC from the basic mechanical flight control system is impossible. As the Safety Pilot is not able to recover the aircraft in case of unintended EFCS commands which might lead to a catastrophic accident, this failure condition shall be extremely improbable leading to a probability of occurrence for this failure condition of $<10^{-9}$. The disconnect function has to be developed according to DAL A [4].

8. Conclusion

This paper provides an overview on the design process of the Experimental Flight Control System (EFCS) for the new DLR testbed ISTAR. It explains the underlying safety concept of the aircraft which forms the basis for its application for the rapid inflight testing of uncertified flight control software. The safety concept and the operational concept of the aircraft with access to the primary flight control system were presented. One important requirement is that the EFCS can be active during landing and take-off as well as in the high-speed regime. Due to this requirement further safety-relevant systems are necessary, as the assumed Safety Pilot's reaction time is not short enough to prevent hazardous or catastrophic events. The safety requirements for these functions have been derived from a Functional Hazard Assessment (FHA). The system architecture for the EFCS was presented. First results of the design considering the safety requirements obtained from the FHA was discussed. The next steps are the definition of Design Assurance Levels for each component or system and required redundancies for systems and interconnecting signals. The interface of each component will be finally defined leading to the preliminary and critical design reviews of the aircraft modifications.

9. Contact Author Email Address

mailto: dominik.niedermeier@dlr.de

10. Copyright Statement

References

[1] Giese, K., Heider, J., and Niedermeier, D., “ISTAR Configuration 2 and 3 Operation and Safety Concept,” DLR-ISTAR-001, 21 Dec 2020.

[2] European Union Aviation Safety Agency, *Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes. CS25*, 24 Nov 2021.

[3] Giese, K., Guerrero Santafe, J., Heider, J., Leißling, D., Neurath, Christian, Niedermeier, et al., “ISTAR Configuration 2 High-level Technical Requirements,” DLR-ISTAR-006, 24 Jan 2022.

[4] SAE Aerospace, “Aerospace Recommended Practice: Guidelines for Development of Civil Aircraft and Systems,” ARP4754, 1 Dec 2010.