Functional hazards assessment of an integrated flight control system validation using model-based design

A Savelev¹,², N Lituev² and E Olidaev²
¹Faculty of Robotic and Intelligent Systems, Moscow Aviation Institute, 4 Volokolamscoe Schosse, Moscow 125993, Russian Federation
²Automatic Flight Control Systems Department, Irkut Corporation, 68 Leningradsky Avenue, Moscow 125315, Russian Federation

Abstract. Functional Hazard Assessment is the beginning of the work on the system safety assessment and it directly affects the design, safety and final cost of the project. Errors in the Functional Hazard Assessment can lead to insufficient system safety or unreasonably expensive development. The main purpose of the work is to introduce the Functional Hazard Assessment validation process which minimizes the risk of incorrect development of MC-21 aircraft Flight Control System. To achieve this goal, Model-Based Design methods are used as validation methods. The time benefit in detecting and isolating errors in algorithms and software with the help of the Model-Based Design is shown. Integrated Flight Control System which includes fly-by-wire control system and automatic flight control system of the Irkut’s airliner MC-21 safety requirements validation process using means of Model-Based Design is considered. As a result of the work, Integrated Flight Control System models were adapted for assessing functional hazards, and a user interface was developed for the flight crew to participate in the simulation of the failures.

1. Introduction
Nowadays, due to the MC-21 project approaching certification phase more tasks connected with safety documentation release are conducted. The Functional Hazard Assessment (FHA) is one of the main documents, which must be carried out before all safety analysis [1].

The FHA is used to assess the impact of the aircraft function failures on the aircraft and its occupants considering existing or assumed mitigation means and derive safety requirements for the aircraft design [2]. The purpose of the FHA is to clearly define each failure condition along with justifying their classification by criticality [3].

Previously, the safety assessment process in Irkut Corporation, consists in the developing, the updating and the verification of safety requirements at the same time as the MC-21 design as required by SAE ARP 4761. From the aircraft level the requirements descend to the Flight Control System (FCS) and Automatic Flight Control System (AFCS) level (“top-down” process) and are supplemented with derivatives according newly identified end effects (i.e. newly functional hazards) from Failure Mode and Effect Analysis (“down-up” process) of each component of Integrated Flight Control System that includes FCS and AFCS.

The main problem of carrying out the FHA is the lack of regulatory procedures and accepted processes for validating the classification of the requirements, according to the criticality of each failure condition. The relevance of this problem is connected with the fact that the validation materials
(including the validation of safety requirements that are the result of the FHA) should be prepared during certification [4]. Validation documents (procedures and results) of the FHA thus should be prepared by the request of a certification authority.

Depending on the expected criticality of a functional failure safety requirements are formed, using the Failure Tree Analysis (FTA) and budgeting. These safety requirements include assignable Development Assurance Levels for functions (FDAL) and items (IDAL), which are responsible for these functions. Also, the required minimum allowable probabilities of occurrence of failures of system elements are included in the safety requirements.

Requirements for independence are based on the rigidity of DAL and directly affect the final cost of the project, the necessary time and labor.

An incorrect assumption of the fail severity thus requires making adjustments in the design at the later project stages (bench / flight tests):

- The product satisfies safety requirements, but inadequately expensive; there is a risk of reduced demand in favour of more affordable competitors;
- The product does not satisfy the safety requirements; redesign is required, which entails a delay in the production, certification and delivery of the developed system.

In order to exclude the possibility of incorrect determination of the criticality of a failure, it becomes necessary to validate each failure condition. One of the validation methods is mathematical modeling. If the mathematical models reflect the behaviour of the systems under consideration and their interactions with the sufficient accuracy, these models can be used to determine the effect of failure on the stability and controllability of the aircraft. It is also possible to assess the failure situation by the flight crew with the help of pilot control simulators. Simulation with a pilot in the loop also allows to evaluate the available methods for recognizing failure and neutralizing actions. To obtain adequate results, models must be developed correctly. Model-based design allows to do this.

Model-based design (MBD) at present is becoming more widespread in a development: in the Aeroengine Control System [5], Intelligent Dynamic Systems [6], Modular Inspection Equipment Design for Modular Structured Mechatronic Products [7]. MBD allows identifying requirements violations and finding software errors in the early stages of the developed product.

The article proposes the use of a new method from a scientific and engineering point of view in the FHA requirements validation - the MBD approach. Integrated Flight Control System (IFCS) of the Irkut’s airliner MC-21 safety requirements validation process is expected to be improved and accelerated by the usage of the MBD. For this, the following tasks need to be solved:

- Confirmation of the applicability of the MDB for the FHA validation;
- Development of a software for a modeling bench;
- Setting up work with real-time simulation equipment using pilot control simulators;
- Determination of quantitative criteria for failure conditions.

2. Methods and materials

To use the results obtained with the help of the MBD, the models of the IFCS and associated equipment must be reliable, that is, similar to real equipment on board the aircraft. The correctness of validation results must be proven. To prove this, the necessity and sufficiency of detailing IFCS models and associated equipment should be demonstrated. The equipment used as pilot controls should be identical to the real one so that the operator (engineer or pilot) can perform similar actions that are performed on board the aircraft. The actions of the pilot (if the pilot is in the aircraft control loop) must comply with the Flight Crew Operations Manual (FCOM) and take into account the problems of the human-machine interface, such as the time to recognise and parry the emerging failure situations.

2.1. Applicability of model-based design to FHA validation

The model-based design approach consists of designing models using elementary blocks and using these models as a basis for the development of embedded software. This means working with models as opposed to working with code (e.g. debugging, designing the architecture, reducing the complexity,
testing) and generating the code from them. This approach aims to reduce the costs associated with testing. Using a model-based design approach makes it easy to create tests associated with a model at the early milestones. Powerful tools which are widespread nowadays allow generating tests automatically, thereby making it easy to test the development of your embedded software early and robustly. Model-Based Design is transforming the way engineers and scientists work by moving design tasks from the lab and field to the desktop. When software and hardware implementation requirements are included, such as fixed-point and timing behavior, you can automatically generate code for embedded deployment and create test benches for system verification, saving time and avoiding the introduction of manually coded errors [8].

The applicability of the MBD approach to the validation of the criticality of IFCS FHA is achieved taking into account the detailed study of the necessary components - internal and interface.

The algorithms that are used in the model are identical to those that are verified in flight tests of the MC-21 aircraft with the participation of EASA [9]. This allows engineers to get the most relevant data from the simulation results. Detailed actuators models of the integrated control system are also used: a set of electro-hydraulic actuators of ailerons, elevators, rudder, spoilers and speed brakes, flaps and slats actuation systems and electromechanical stabiliser actuator. These models also take into account reconfiguration of the system in case of failures of active actuators on the surface. Models of complex avionics systems, chassis and engine operation provide a sufficient level for validation of IFCS FHA. The model of the AFCS mode control panel (AFCP) is also included. It takes into account time delays in generating and transmitting signals, and furthermore is fully in line with the real AFCP logic of switching and indication of modes on AFCP indicators. Various weather conditions could be set thanks to complexity of the model and flexibility of simulation preferences. This ensures that the FHA is carried out for the worst conditions. The development of models at this level of complexity is a necessity for ensuring the validation of IFCS requirements.

There are some sufficient conditions that should be met to use the MBD approach, such as application of the methods for managing the configuration of the model (including tracking changes in models, integration of FBW and AFCS models). Moreover, the convergence of models, current software (used at the semi-natural test benches) and flight test results with current software and real actuators are also required. Convergence analysis showed that the implemented models are adequate for researching problems connected with the behaviour of FBW and AFCS in normal and failed flight conditions. Correct configuration management of the model ensures the use of current versions of algorithms and software.

2.2. Functional diagram of the mini test bench
MATLAB Simulink is used as the modeling environment, as the most progressively developing software package today for solving such problems. Mathematical models of an IFCS, interacting systems, and aircraft flight dynamics were prepared using the standard libraries built into MATLAB Simulink.

Interaction with visualisation and indication tools (Flight Ind, Flight Gear) and fault input interface (Fault Input Panel) is performed via UDP (Universal Datagram Protocol). This protocol allows for the exchange of information between components of the test bench without affecting the speed of modelling. Furthermore, as UDP is a network protocol, separate machines in a local network could be used for different human-machine interface implementation or even for simulating different systems. This allows improving the test bench with the help of distributed calculations.

AFCP is developed using the Qt cross-platform software libraries and connected to MATLAB Simulink in the same way using UDP to increase user convenience and information processing speed. The IFCS Fault Input Panel is similarly configured interface, which includes the ability to disable one or more actuators on the surface, hydraulic and electrical system failures, as well as other related FHA failures.
Interaction with physical pilot control simulators (Sidestick Unit, Throttle Quadrant Assembly, Pedals Control Unit) is carried out using the appropriate drivers and FlightSim library for MATLAB Simulink.

The resulting complex test bench was configured for modelling both in real time and in the “accelerated” time modes for solving various types of problems.

Real-time simulation allows you to conduct a flight assessment of the criticality of the situation at the employee’s workplace, since the available simulators of the pilot controls and visualisation bodies ensure that the employee has a correct understanding of the system’s behaviour and the impact on safety and flight in general. At the same time, in the evaluation process, it is possible to quickly change the logic or algorithms of the developed system component by adding, disabling or switching blocks from the MATLAB Simulink library. There is no need for time and financial costs thus that occur during the similar validation on test benches with real flight computers and a real aircraft, requiring a “flashing” of the software when making any changes to it.

Simulation in “accelerated” time allows performing validation in cases where an assessment of a given situation is necessary with a large number of initial conditions. This problem can be solved when assessing the consequences at different stages of flight, under different weather conditions (wind, wind shear), abnormal configurations that exacerbate the impact on safety (failure of various hydraulic systems or electrical systems, engines). If the necessary test vectors are correctly prepared and the simulation is launched in a cycle, the engineer or pilot does not need to conduct simulation of each case step-by-step, he only has to monitor the progress of the simulation, performing other tasks in parallel, and analyse the results in the end of the simulation. A special checklist for assessing the flight situation and the impact on safety is used in modelling in “accelerated” time. This approach has also found application in validating the functional requirements for FBW and AFCS.

Besides traditional testing, that involves simulating different flight scenarios, complex modelling system allows performing a kind of laboratory tests, such as frequency analysis. This kind of research is needed to prove aeroelasticity stability, one of the most important characteristics of an airplane. Traditionally these tests are carried out on a real aircraft using laboratory equipment, so there is no possibility to perform tests with a full range of initial conditions (due to the costs of prototypes destruction). Performing frequency tests on the complex model allows receiving more credible results than analytical (mathematical) method results that takes into consideration only simple linear models. At the same time all ranges of frequencies and amplitudes could be tested without danger of destruction. As it was said before, MBD approach gives engineers tools to tune the system to satisfy frequency criteria in their workplaces.

As it can be seen from the description above, the developed modelling system in terms of simulating controls and software is currently widely used. As a result of, the means of integrating various components of the “mini test bench” became available not only to the programmer, but also to the control system engineer. The development of such kind of system thus does not require the involvement of third-party companies and additional financial investments. An assessment of safety and flight situation is adequate and can be used to make adjustments to the relevant sections of the FHA.

The functional diagram of the test bench is shown in figure 1.

2.3 Comparing results with criteria
At the end of the simulation, it is possible to assess the consequences of failure. The criteria available in regulatory documents [1] are qualitative:

- Catastrophic (CAT): risks which would result in multiple fatalities, usually with the loss of the aircraft.
- Hazardous (HAZ): risks which would reduce the capability of the aircraft or the ability of the crew to cope with:
  - A large reduction in safety margins or functional capabilities,
  - flight crew cannot perform their tasks accurately or completely due to physical distress or excessive workload,
Figure 1. The functional diagram of the mini test bench.

- serious or fatal injury to a relatively small number of the occupants other than the flight crew.
  - Major (MAJ): risks which would reduce the capability of the aircraft or the ability of the crew to cope with:
    - a significant reduction in safety margins or functional capabilities,
    - a significant increase in crew workload or in conditions impairing crew efficiency,
    - discomfort to the flight crew,
    - physical distress to passengers or cabin crew, possibly including injuries.
  - Minor (MIN): risks which would not significantly reduce aircraft safety, and which involve crew actions that are well within their capabilities. Minor risks may include, for example, a slight reduction in safety margin or functional capabilities, a slight increase in crew workload or some physical discomfort to passengers or cabin crew.
  - No Safety Effect (NSE): risks which would not impact the safety of the aircraft.

Qualitative criteria do not allow accurate analysis of the modeling results. For accurate analysis, quantitative criteria based on qualitative classification have been developed. These quantitative criteria take into account stability and controllability, as well as structural strength of the aircraft.

Comparing each characteristic obtained during the modeling with the criteria, the correct criticality of the failure condition is determined. The proposed failure validation method allows us to determine at the functional level the actual criticality of each violation.

3. Results and discussion
Regulatory documentation does not govern the validation of functional hazard assessments. The authors suggest validation of failure situations for fear of the possible misjudged criticality.

Regulatory documentation [1-4] does not provide clear quantitative criteria for determining the degree of criticality of a hazard. Therefore, some failure conditions in the IFCS FHA can be assessed
inadequately. Therefore, based on the qualitative criteria, quantitative criteria have been developed that take into account stability, controllability, and also aircraft strength.

The authors analyzed the experience of a model-based design of aircraft systems [5] and other technical systems [6, 7]. According to the analysis of the available tools, the MATLAB was chosen as a main IDE.

As a result, a mini test bench was developed, quantitative criteria for FHA, as well as methods for using the stand both in real and accelerated time.

The IFCS MC-21 FHA has become the result of the work. The results of FHAs validation have allowed accelerating the work without using common test benches with real equipment. MBD has reduced the financial costs of FHA carrying out.

The software and hardware complex that has been implemented is generally universal. The experience gained in the construction and debugging mini test bench will significantly reduce the time for developing new projects in the future due to the gained experience and well-established processes when working with such models.

Based on the validation results, the criticality of functional failures identified during the previously performed FHA was clarified. In accordance with the safety process [1, 3], these refinements will be included in the design process.

The obtained result proves that the MBD can be used in the validation of FHA at aircraft and FCS levels of abstraction.

Currently, this approach, in addition to early detection of design errors, can also reduce the time spent on large stands.

Further work in this direction should be aimed at improving the quality of the model in terms of avionics (developing more detailed system models), as well as the introduction of MBD at the aircraft level. To spread the model-based design approach to the Irkut Corporation, significant cooperation of all interested departments is required. The tasks of storing, processing and detailing large volumes of information should be solved. Many related tasks, such as configuration management, model validation (convergence analysis), will also arise and need to be addressed.

For the successful functioning of MBD, the methods and standards of Irkut Corporation must be developed and approved, which will allow using these materials in the certification of new types of aircrafts. This is the perspective ways for future projects in this area.

4. Conclusion

MBD is a real and effective way in the validation of FHA, which is confirmed by the validation of IFCS MC-21 FHA. A number of necessary tasks were solved to use of MBD in the validation of IFCS FHA - integration of software and hardware complex modelling system based on MATLAB Simulink, an analysis of model convergence with existing software and equipment on test benches and aircraft was carried out, a model configuration management process was developed.

The implemented mini test bench reliably fulfils tasks both in real-time modelling, the main purpose of which is the possibility of direct flight assessment of the situation, and in “accelerated” time for stream-based solution of similar problems under various conditions.

Work with the model is carried out both with the participation of pilots for accurate assessments of the flight situation and the impact on safety, and is available to the engineer of the automatic control systems department. The developed criteria for assessing the impact on safety make it possible to analyse the simulation results according to the characteristics of aerobatic and navigation information (such as roll angle, lateral and normal overload, pitch angle, angle of attack, glideslope angle and many others).

The results FHA validation with the use of MBD has become the IFCS MC-21 FHA, which will be submitted for certification of the aircraft.

Currently, the safety assessment process in Irkut is improved compared to the requirements of SAE ARP 4761. This process includes the developing, validation, updating and verification of safety requirements.
Acknowledgments
The authors are grateful to the Irkut Corporation for the publication of this article and support for using modern methods of designing flight control systems.

References
[1] European Aviation Safety Agency 2007 Certification Specifications for Large Aeroplanes CS-25 Amendment 3
[2] Bieber P, Metge S, Morel M, Ple J 2019 Aircraft Safety Model Development and Integration in a Risk Observatory. EASN International Conference on Innovation in European Aeronautics Research (ONERA, Université de Toulouse) https://hal.archives-ouvertes.fr/hal-02078264
[3] SAE ARP 4761 1996 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment (SAE International) p 311 https://doi.org/10.4271/ARP4761
[4] SAE ARP 4754 2010 Guidelines for Development of Civil Aircraft and Systems (SAE International) p 115 https://doi.org/10.4271/ARP4754A
[5] Zhanga D, Luab J, Wanga L and Lia J 2015 Research of Model-based Aeroengine Control System Design Structure and Workflow. Proc. Eng. 99 788 https://doi.org/10.1016/j.proeng.2014.12.603
[6] Oestersötebier F, Abrishamchian F, Lankeit C, Just V and Trächtler A 2016 Approach for an Integrated Model-based Design of Intelligent Dynamic Systems Using Solution and System Knowledge. Proc. Technology 26 436 https://doi.org/10.1016/j.protcy.2016.08.056
[7] Lukei M, Hassan B, Dumitrescu R, Sigges T and Derksen V 2016 Modular Inspection Equipment Design for Modular Structured Mechatronic Products – Model Based Systems Engineering Approach for an Integrative Product and Production System Development. Proc. Technology 26 455 https://doi.org/10.1016/j.protcy.2016.08.058
[8] Why Use Model-Based Design? available at: https://www.mathworks.com/solutions/model-based-design.html
[9] EASA flight test experts completed the second session of certification flights, available at: http://eng.irkut.com/press-centre/news/2392/