

METHODS OF ASSURING THE FUNCTIONAL SAFETY OF AIRCRAFT ON-BOARD INSTRUMENTATION & CONTROL SYSTEMS IN THEIR LIFE CYCLE

Aleksandr KHARYBIN and Viktoriya POHYL

Abstract: This paper describes an approach for assuring the functional safety of perspective aircraft on-board Instrumentation & Control (I&C) systems on the basis of reconfigurable computation nodes (CN). The functional-architectural model of aircrafts on-board I&C systems with possibility for CN reconfiguration, as well as enhanced method for assuring the functional safety of aircrafts on-board I&C systems on their design stage and a new method for assuring this feature during the operational stage of such systems, based on the proposed model and which consider the on-line criticality and reliability control results of certain elements and functional subsystems is proposed and discussed.

Keywords: On-board Instrumentation and Control System, I&C, Functional Safety, Assurance Method, Computation Node, Reconfiguration, Functional-Architectural Model.

Introduction

Modern tendencies to development the critical application information and control systems (I&C) evidence, that the role of On-board I&C Systems of multipurpose aircrafts, which use the advance informational technologies and microelectronics achievements, impetuously increases. They lay the great responsibility on such Aircraft On-board I&C Systems (AOBI&CS) for successful flight (right up to completely suspending the human from flight control),¹ that, on the one hand, is connected with the necessity for implementation the continuous functionality control level of all the subsystems of AOBI&CS's and an aircraft in whole, automatic implementation of all or main flight stages, and on the other hand – with the necessity to control pilots state and traffic situation around an aircraft and its location in it. Taking into consideration the abovementioned, one of the main requirements, set forth for the computing subsystems, used as a part of AOBI&CS's for assuring the implementation of all control

algorithms and necessary computations, is the assurance of their high-level reliability, survivability and functional safety.

Failure of individual sensors, actuators, computation blocks, data exchange channels (“aircraft-surface” and intersystem), as well as the subsequent loss of computational power (performance) and other information sources on condition of the controlled object (aircraft and its subsystems) should not lead to the disastrous effects for the system as a whole or for its environment. That is why there is an exigency in permanent control and management (improvement) the functional safety level in case of its degradation lower, than its is specified in the Technical Specifications.

Based on reviewing the literature on analysis, evaluation and assurance of AOBI&CS functional safety² and analysis and evaluation methods of AOBI&CS’s functional safety on subsystem (element) criticality level,³ we introduced a functional safety assurance method for the AOBI&CS’s at the design⁴ and other stages of their life cycle⁵ from a structural perspective that does not separately consider components as software and hardware tools.

The objectives of this article is to describe the approach for assurance the functional safety of AOBI&CS’s, based on construction of its computing subsystems on the ground of unified reconfigurable computation node,⁶ new functional-architectural model of such AOBI&CS, improved functional safety assurance method of I&C system of this class on their design stage, as well as to describe the new method for assurance the functional safety of AOBI&CS’s on their operation stage, which allow to consider the criticality levels for implementation the aircraft safety related functions of different elements and subsystems, which form the AOBI&CS’s, extent of possible damage to the AOBI&CS’s and aircraft in whole at origination of a situation, connected with a failure of any separate elements/subsystems or the on-board I&C systems in general and the risk, associated with this.

For the successful implementation of requirement to the functional safety of AOBI&CS it’s necessary to continuously control and support the values of the corresponding parameters within the prescribed limits, and in case of their values deviation from the accessible region – to implement activities for bringing them (by restoration using the computing subsystems reconfiguration) to the preset (maximum possible in a definite situation) functional safety level or to support the minimum necessary level of the mentioned feature for saving the safe functioning conditions of the controlled object (aircraft) and eliminating the possibility for occurrence the disastrous situation for it and its environment (objects on earth/sea or other aircrafts). The following particular scientific-technical tasks are pursued:

- to propose and to describe, using the correspondent mathematical model, the architecture functioning of the perspective AOBI&CS's with the reconfigurable computing subsystems CN the consists of computation modules;
- to enhance the earlier proposed method for assurance the functional safety of the AOBI&CS's on their design stage based on the AOBI&CS model with reconfigurable CN and considering the criticality level of the individual elements, which form its functional subsystems;
- to develop a new method for assurance the functional safety of the AOBI&CS's on their operation stage basing on the received model of the reconfigurable node and considering the results of the criticality on-line control, results of reliability and functional safety of individual subsystems of the AOBI&CS's (information and control flows) and their forming elements.

AOBI&CS's Functional Safety Assurance using Reconfigurable Computation Node

In order to assure the control of the information and control processes functional safety level in the AOBI&CS and its safety related subsystems, it is suggested, at the organization of perspective AOBI&CS's, to use "flexible" data-computing architecture, given on Figure 1, which is based on using some Computation Node with a possibility for architecture flexibility based on the reconfiguration in case of failures and/or operation errors of the unified (on performance and functions) computation modules, which have multiple version structure on the circuit decisions, used for their implementation, radioelectronic component structure and software (SW) tools.

This approach for the AOBI&CS's design will allow to assure the functional safety of its On-board I&C Systems, established by aircraft regulatory documents and technical specification, only on the assumption of operating the high-reliability optimization subsystem of computation architecture and performance in the mentioned Computation Node (CN) at the support of the necessary multi channel processing of allocated information and control processes, implemented in the interests of all, but in the first place – the most critical (from the aircraft functional safety point of view) functional subsystems.

To solve this task, at the R&D stage for creating the perspective AOBI&CS , it is necessary to develop a specialized firmware for the information technology (IT) optimization the distribution redundancy rate of critical computational process in the given AOBI&CS CN, as well we IT for assuring the functional safety of On-board I&C subsystems, which algorithms should be implemented by a high reliability reconfiguration server in the so called "hard Real Time Mode."

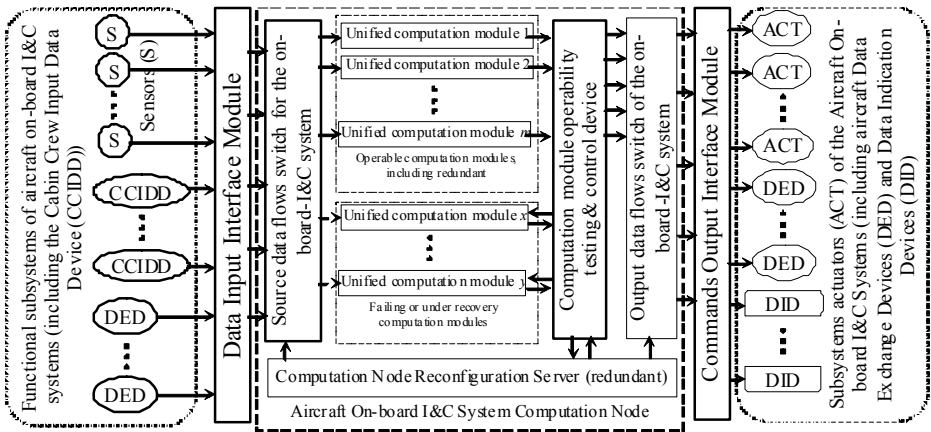


Figure 1: Simplified view of the “flexible” computing subsystems architecture of prospective AOBI&CS’s with the possibility for increasing their functional safety by reconfiguration.

Development of perspective IT for assurance (enhancement) the functional safety of AOBI&CS’s, within the process of preflight preparation and while different flight stages of an aircraft, is a complex task, which salvation depends on individual aircraft type and its On-board I&C System architecture. At this it is determined, that such IT should operate on the basis of digital I&C system CN reconfigurator, which consists of the reconfiguration sever (with corresponding system and application SW tools), highly reliable switches of input and output (control) data flows, and system elements for operability control (testing) the unified computation modules (CM) out of the AOBI&CS CN structure; the respective relationship chart is in Figure 1.

In order to describe the functioning process as well as to implement the express-evaluation and forecasting the reliability and operability level of the computing subsystem of AOBI&CS with the proposed architecture on the basis of CN with the high reconfiguration capabilities it is reasonable to use the continuum functioning model of the AOBI&CS CN.⁷

The task for AOBI&CS functional safety assurance on the operation stage may be solved on the basis of the proposed approach thanks to prevention of all the dangerous failures (errors) in On-board I&C System CNs operation or their consequences development (elimination) control to minimize operability harm of the most critical for the aircraft functional safety On-board I&C subsystems. Thereby, the intellectual “core” of the perspective embedded subsystem for assuring the discussed feature of AOBI&CS’s should be the Decision Support System (DSS) on the IT basis on assurance the given or maximum possible, in the specific situation, reliability level and

functional safety of AOBI&CS. The described CNs AOBI&CS'sW should be designed on hierarchical principle and should have four levels (see Figure 2):

- reconfiguration level – represented by the control software, implementing the continuous operating monitoring of the AOBI&CS CN in real time mode and forecasting possible conditions (parameters) change of the AOBI&CS CN and its individual subsystems, as well as assuring the possibility for reconfiguring the AOBI&CS CN on corresponding flight stages at given factors of reliability, criticality and functional safety of individual subsystems and the On-board I&C System in whole;
- level of aircraft navigation and AOBI&CS's operability control – the level of the integrated software tools, which assure AOBI&CS's, operability control, aircraft position in space and operation of the navigation circuit (control of these subsystems);
- level of the functional subsystems of AOBI&CS's – level of the functional software tools, which implement salvation of definite tasks on determining the aircraft orientation in airspace, propulsion control, aircraft mechanics and its other subsystems;
- control and manipulation signals processing level – level for control the devices and mechanisms of functional subsystems of AOBI&CS's, which are responsible for analog-to-digital and digital-to-analog conversion of sensors electric signals and actuators control commands, coding/decoding the control commands and information from/for external (including the ground) services and systems, as well as for solving other simple data-computing tasks.

AOBI&CS CN should also has an adaptability property for assuring the safe AOBI&CS's functioning in whole during the process of their operation (static reconfiguration) at changing the requirements to the reliability values and functional safety. At this the AOBI&CS's CN adaptation, as a rule, is based on the following types of reconfiguration:

- structural, contained in computing system structure reconfiguration, consisting of the computing modules entered into its structure, which assure the operation of a definite subsystem or group of functional subsystems of AOBI&CS's;
- architectural, contained in changing of algorithms and level of the computational processes distribution by changing the operating software content and structural interrelation of computation modules within AOBI&CS's Computation Node;
- time, that allows to use temporal redundancy of individual processes for increasing the validity and/or accuracy of computational results or for capacity

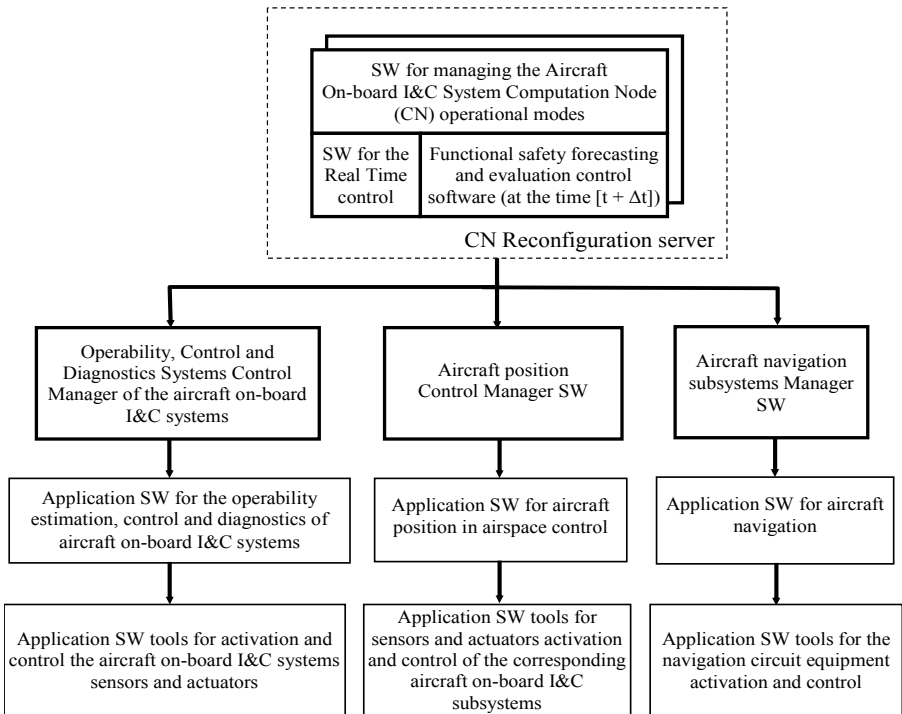


Figure 2. Reconfigurable AOBI&CS's CN software structure.

enhancement in the interests of other computational process (task) which, as a rule, has a higher priority (criticality) from the functional safety point of view.

Functional- Architectural Model of the AOBI&CS's

For researches of reliability and functional safety of AOBI&CS at the process of its functioning with a glance on the peculiarities of functional and architectural design of the considered system, as well as for defining the operability impact level of software tools and computation modules hardware components on the whole functioning safety system, it is necessary to represent its Functional-Architectural Model (FAM), which general view is given on Figure 3.

The given model is considered from the position of component approach, which essence is as follows:

- system is represented as a combination of interacting functional blocks, which structure consideration level gives a possibility to receive reliability evaluations and, consequently, functional safety, i.e. gives the possibility to

determine the disastrous impact of functional blocks failures on the system operability;

- the system is examined on the architecture level, that represents software and hardware components and describes their interaction.

This model of AOBI&CS gives a possibility to determine general logic organization of I&C system, that allows to distribute the functions on its structure components, to determine the interaction methods and principles of hardware (technical) tools and software.

Functional-Architectural representation of AOBI&CS's reflects the interaction of hardware (HW) and software (SW) tools as two basic components of any modern

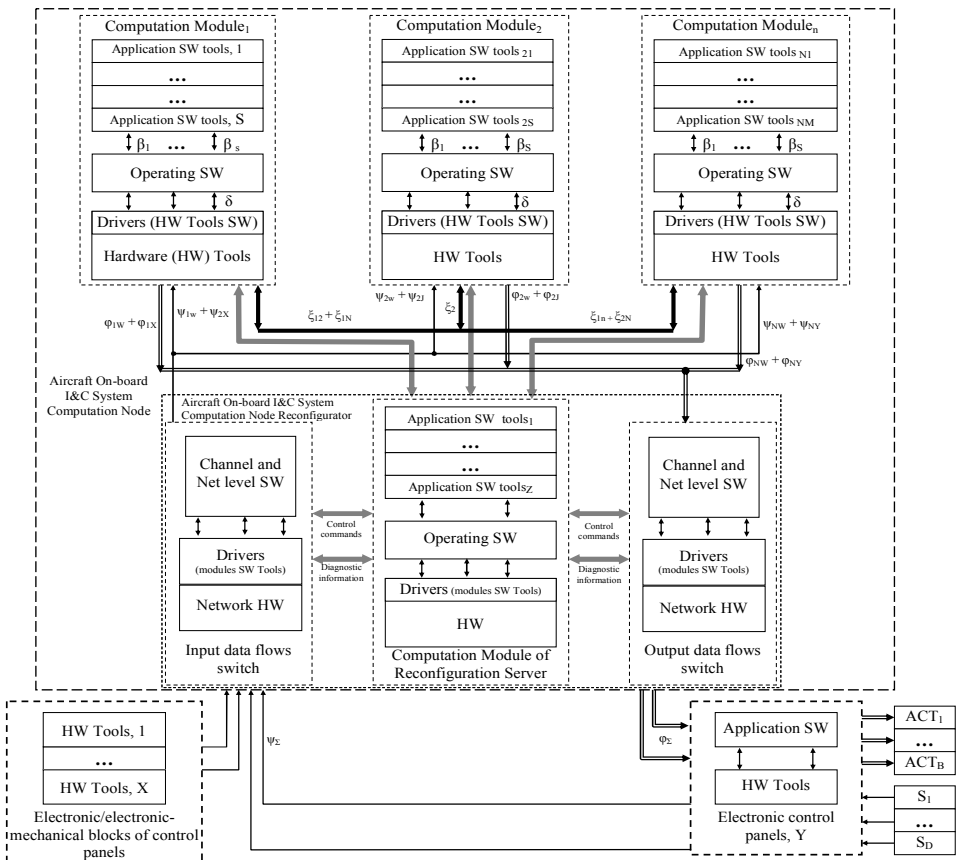


Fig. 3. Simplified Functional-Architectural Model of AOBI&CS with reconfigurable Computation Node.

I&C system, which may be specified and described by the system of corresponding varieties, which general view is given below:

$$\left\{ \begin{array}{l} HW = \{N, B, A, D, Y, X\}, \\ SW = \{OSW, ASW\} \end{array} \right\},$$

where N – set of Computation Modules in AOBI&CS CN structure; B – set of AOBI&CS sensors; A – set of AOBI&CS actuators; D – total productivity of the Computation Node, Y – set of On-board I&C System electronic control blocks; X – set of electronic/electronic-mechanical modules of On-board I&C System control panels; OSW – operational software; ASW – set (package) of the application software tools.

Interaction between the application software (AppSW) and operation SystemsW (OS SW), as well as between OS SW and corresponding to it hardware (HW) tools may be assigned by the intensity of data exchange (interaction) or by the intensity of sessions requests. At this, each operable condition of the discussed AOBI&CS (its separate subsystem) on individual operational stages (pre-flight preparation, takeoff, en-route, landing, taxiing) in normal (specified) operating conditions will correspond to its own parameters system, describing the data exchange intensity values (signal interaction, sessions requests) or to the bandwidth of the used data exchange buses (channels) of $\{\beta_s, \delta, \xi_N, \varphi_{NW}, \psi_{NY}\}$ type.

Thereby, having such data on real values of the given parameters, which describe the separate elements of informational interaction of AOBI&CS (its subsystem) functional-architectural model, as well as on acceptable deviation of their instantaneous values from the averaged, earlier determined values it is possible, by comparison, to implement the operability express-evaluation of given object, to reveal the places which have discrepancies and take appropriate measures for assuring the restoration of examined system normal operation.

This approach allows to implement the rough functional safety evaluation on AOBI&CS operability (functioning) level, and to study the interaction order at functioning elements, included in the architectural models of the like system more precisely. At this, the proposed model has limits, connected with the fact that at consideration the functional order of separate elements of AOBI&CS 's architecture and its subsystems, some nonrelevant failures (errors) of operational SW work and separate application software tools, which influence on calculations accuracy, and therefore on the final decisions and control signals conditioning that may be the consequence of software or on-board I&C system, as a whole, design defects, not revealed at testing, verification and validation stages and may be the reason for the new defects occur-

rence (including interaction of separate architecture elements), that may lead to the significant decreasing of the evaluated systems (subsystems) functional safety level.

To implement all the actions, necessary for achieving the required safety integrity level of the safety related systems on the systematic base, in the standard a model of the complete safety life cycle of complex technical safety related E/E/PE system is assumed as a technical base. Consideration and calculation, within the limits of the mentioned AOBI&CS life cycle model researches, as a safety related E/E/PE, allows to separate the main stages of its life cycle from the view of assurance the necessary (specified) level of its functional safety. This allows to enhance the adequacy of existing models and analysis (evaluation) methods analytical survey and assurance the mentioned property of the specified safety related class, as well as to taper the field of researches to achieve the greater reliability of questions examination on enhancement the existing and, if necessary, developing of new assurance methods of the given level of considered reliability properties and designed On-board I&C System functional safety.

AOBI&CS's Functional Safety Assurance Method at the Design Stage

Design management is an important process of risk management and functional safety of the designed I&C systems, which allows to assure their development at assurance the specified properties level. Design management includes establishment of design rules and guidance's for assurance the safe operation, allocation of functional blocks, modularity assurance, facilitation of assembling and providing the on-board I&C systems warranty services, and allows assuring their correspondence to the requirements.

The main point of the proposed AOBI&CS's functional safety assurance method is to achieve the maximum efficiency from the following groups of measures:

1. Increasing the reliability and stability of the data-computing processes in the subsystems of on-board I&C systems which implement the safety functions by introduction the algorithmic, technical, time and other types of redundancy;
2. Utilising new technological decisions for the elements, which have the maximum multiplicity values of criticality on the functional safety analysis results of the given critical subsystem in order to increase their reliability;
3. Changing of the structure-architectural or algorithmic organization of the most critical data computing processes in AOBI&CS's to reduce the criticality multiplicity values of the elements, included in the critical subsystems of on-board I&C systems. At this, it is necessary to try to get the minimiza-

tion of multiplicity criticality values for the elements, which have the lowest quantitative values reliability indexes and/or maximum values of criticality multiplicity in the subsystems.

On results of measures implementation on enhancement the separate subsystems functional safety and AOBI&CS's in whole the evaluation of the given feature is performed and the difference in the received values risk indexes and each functional safety critical function is determined, following which the efficiency of decisions is analyzed. The simplified algorithm of functional safety assurance method of on-board I&C systems on the design stage is given on Figure 4.

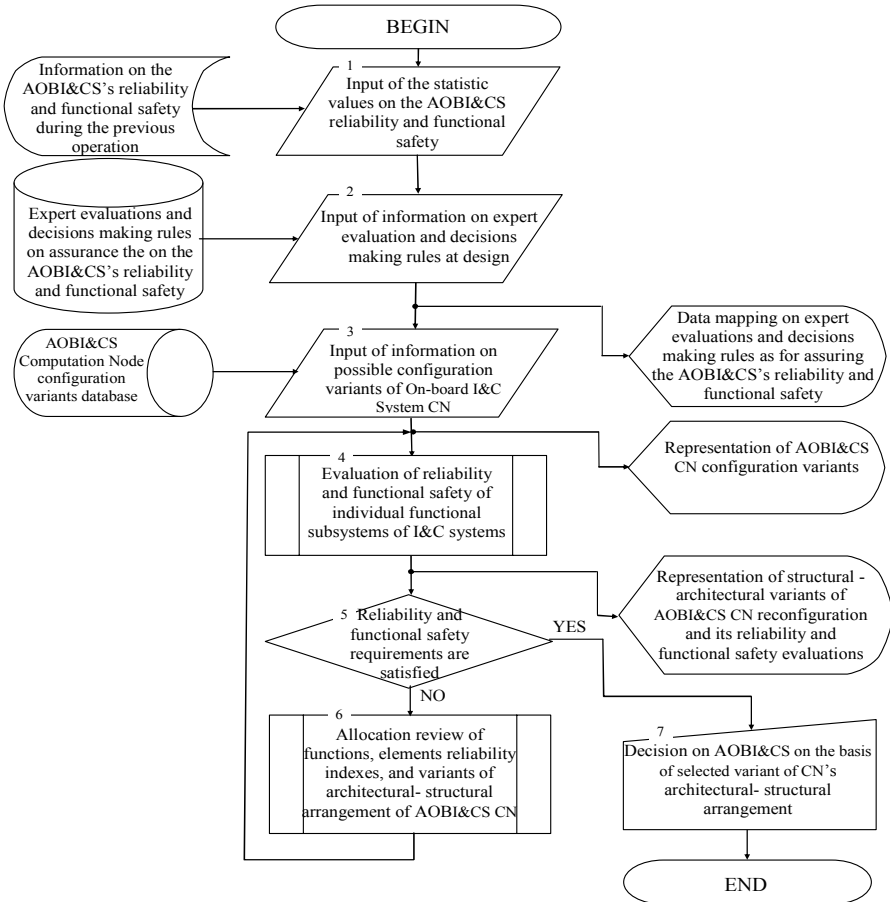


Figure 4: Simplified algorithm of functional safety assurance method of the AOBI&CS's on the design stage.

Assurance of subsystems reliability and functional safety of on-board I&C systems on the design stage should be as well implemented on the following main aspects:

- reliability assurance of the system hardware part and interacting elements;
- reducing spends of the computational resources and information processing time;
- software reliability assurance (operating and application);
- source data validity enhancement and possibility of their receiving in the real time mode.

For reliability assurance of on-board I&C subsystems it is necessary to use high-reliability system elements, reasonable methods and ways for achieving the specified reliability level in respect to the hardware part, as well as their highly qualified assembling and maintenance.

As a result of our previous research on AOBI&CS's functional safety, we received criticality level indexes of individual elements that allow to determine the list of the most unreliable elements in subsystems of on-board I&C. Thus, on the design stage it is possible to take measures for enhancing their characteristics. This is implemented by selection of elements with the largest MTBF, introducing multi-channels into the system (redundancy, diversity) and special engineering solutions except for those obligatory for implementation the designated function (including complete self-diagnostics).

AOBI&CS's Functional Safety Assurance Method at the Flight Stage

Important point in assuring this AOBI&CS feature during the aircraft flight is the assessment of possibility for On-board I&C System reconfiguration (their CN structural-architectural arrangement) and defining the time, when this is possible. If reconfiguration and reallocation of data-computing flows of on-board I&C subsystems are possible and will not lead to the critical violation of On-board I&C functioning, they are implemented automatically. Otherwise, the cabin crew may participate in taking decision on compulsory reconfiguration or on its denial.

Consider the procedure for choosing the variant of AOBI&CS CNs structural-architectural design and computational resource allocation in it, at which the greatest (maximum possible) indexes, characterizing the functional safety of On-board I&C System and an aircraft in whole, may be achieved.

If the AOBI&CS Computation Node, in a certain time period is operating with the specified capability (quantity of computation parallel flows J and quantity of nodes computation modules N). Each Aircraft On-board I&C subsystem is intended for implementing the set of functions $\{F\}$, consisting of a set of critical $\{F'\}$ – safety func-

tions (F_E) and non critical $\{F''\}$ functions. It is apparent that $F' \subset F$, $F'' \subset F$, $F = F' + F''$. Each n function is represented by the set of tasks $\{Z_n\}$, which implementation assures the critical function realization from the set $\{F'\}$.

If $\{J'\}$ and $\{J''\}$ – is a necessary set of parallel computation flows, necessary for processing the critical and non critical functions correspondently. The $\{J'\}$ set is represented by the obligatory quantity of parallel computation flows in AOBI&CS CN for implementation all the critical functions from the $\{F'\}$ set.

The total capacity (Q) of AOBI&CS CN is determined from the formula: $Q = J \cdot N$.

The functioning rules of AOBI&CS CN Reconfigurator at different performance conditions of the CN, which are the results of changing the performance of individual computation nodes out of its structure, are the following.

1. If $Q \geq J' + J''$ so the CNs performance is above or equal to the specified (necessary for the normal AOBI&CS functioning) and the functional safety value (F_s) is within the range of the specified value (see Figure 5), then the CNs resources are used for solving the whole set of tasks from the set of all functions $\{F\}$.

At this variant of AOBI&CS CN structural-architectural design the redundant computation modules will be in the hot standby for the most important critical functions $\{F'\}$, forming, in such a way, the parallel I&C channels in the critical subsystems.

2. In case, if $J' \leq Q < J' + J''$, to assure the continuous and safe operation of AOBI&CS's in whole there should be assured the effective loading and distribution of computational resources in case of these of those computation modules failures.

At this, the necessary condition for distribution of nodes computational resources is a formation of the ranked (on the importance rate of the functions, implemented by

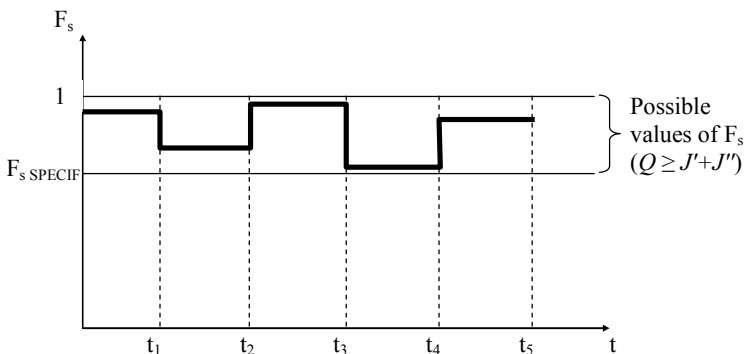


Figure 5: Change of the functional safety index of AOBI&CS at normal operation of CN ($Q \geq J' + J''$).

aircraft on-board I&C subsystems) list of all the AOBI&CS's active functions (in concordance with the current flight stage) as continuously updating table (example is given on the Table 1). At this, the ranking of functions $\{F''\}$ is implemented on the following indexes:

- P_{F_n} – possibility of an operational failure of the n non-critical function;
- v_{BM_n} – criticality level of computation modules, involved in n non-critical function implementation;
- IMP_n – weighting coefficient of importance of n non critical function, determined by the designers.

Table 1. Example of functions $\{F''\}$ ranking table.

	P_{F_n}	IMP_n
f''_1	0.0005	1.0
f''_2	0.0013	0.95
...	0.0011	0.93
f''_n	0.00023	0.91

On the present stage of variant selection of AOBI&CS's CN structural-architectural design for computation the functions $\{F\}$ set, for the purpose of computation resources operational relocation, is implemented, first of all, for the functions from the $\{F''\}$ set, considering the given in Table 1 parameters, provided that all the critical functions ($\{F'\}$ set) are implemented by computation nodes in full scope.

During the CN functioning process it is necessary to relocate the computation resources according to the rule, on which those functions for which the condition $\{P_{F_n}, IMP_n\} \rightarrow \min$ is fulfilled are cancelled first of all.

3. At $J' > Q$, to assure continuous and maximum possible AOBI&CS's safe functioning in general there should be assured the relocation of computation resources in case of computation modules failures. At this the necessary provision for relocation of CNs resources is making the ranked (on importance criterion of functions, implemented by aircraft on-board I&C subsystems) list of all AOBI&CS's active functions (in correspondence with the current flight stage) as a constantly updated table (the example is given in Table 2, the parameters values in the last two columns are displayed for the cabin crew). At this the ranking of $\{F''\}$ functions is implemented on the following indexes:

- $v_{\Sigma n}$ – specific total criticality of n aircraft on-board I&C subsystem, implementing the safety function;

- P_{F_n} – operational failure probability of n safety function;
- U_n – damage, possible at failure the n safety function;
- Fs_{SPECIF} – index value of function safety, given in the technical specification;
- $Fs(t)$ – real value of functional safety index in the time point t ;
- ΔFs – difference between Fs_{SPECIF} and $Fs(t)$;
- IMP_n – importance weighting coefficient of n safety functions, specified on the design stage.

Table 2. Example of ranking table of safety functions $\{F^i\}$.

	$v_{\Sigma n}$	P_{F_n}	U_n	Fs_{SPECIF}	$Fs(t)$	ΔFs	IMP_n
f_1	0.121	0.0078	0.75	0.988	0.993	0.005	1.0
f_2	0.097	0.0012	0.75	0.982	0.985	0.003	0.89
...
f_n	0.102	0.0002	0.5	0.974	0.995	0.021	0.82

Let's consider the concept and process of AOBI&CS's CNs computation resources relocation at the situation of its constituent computation modules element wise failing on the simplified example of its only two, parallel on time, safety functions f_1 and f_2 implementation which time diagram is given on Figure 6.

At the time point t_0 AOBI&CS CN implements safety functions f_1 and f_2 with some unknowns on the results of operating evaluation of functional safety indexes values $Fs_1(t_0)$ and $Fs_2(t_0)$ correspondently, which are numerically greater the specified functional safety level for these functions.

At this, the reconfiguration server control software constantly implements forecasting the functional safety level change of individual functional subsystems for the time point $[t + \Delta t]$ by implementing the evaluation of $Fs_1(t_0 + \Delta t) = Fs_1(t_1)$ and $Fs_2(t_0 + \Delta t) = Fs_2(t_1)$ indexes on the basis of failure condition of one computation module out of the AOBI&CS's computation nodes structure, which are involved in specified functions implementation. This is implemented with the purpose of subsequent optimal computation resource relocation between the specified functions, considering the parameters, given in Table 2.

On the results of functional safety indexes for the forecasted at the time point $[t + \Delta t]$ decreasing the number of operable computation modules out of the AOBI&CS's

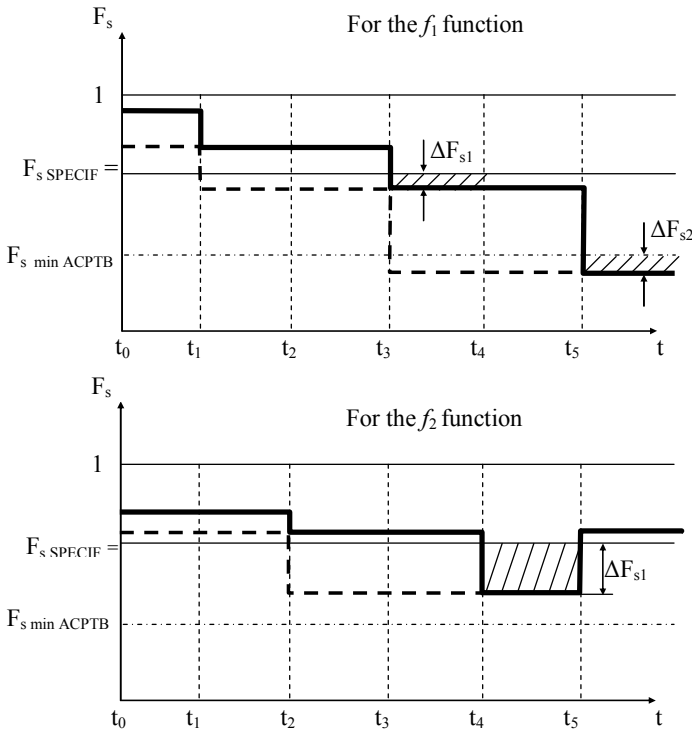


Fig. 6. AOBI&CS functional safety index change during the CN function process at the failure of computation module ($J' > Q$).

computation nodes structure, which are involved in implementation of the specified function, the calculation of odds between the forecasted and specified values of functional safety indexes is implemented – the different of functional safety indexes (ΔF_s), on the reason of that the automatic ranking of AOBI&CS’s implemented functions is performed, at which the more higher positions in the corresponding table are rendered to those functional subsystems, for which the “loss” of a computation module will introduce lesser damage (lower quantitative value ΔF_s) concerning the specified value of functional safety index.

At occurrence the real computation module failure in a AOBI&CS CN the real time control software of reconfiguration server performs the “shutdown” of a data-computing channel for that function, which takes the last line in the ranking table, and on the free channel of the operable computation module there launches the software of that process, which normal operation was “violated” in the result of the mentioned computation module failure. After implementation of the recovery-reconfiguration operation in the interests of more critical function, the control forecasting and evalu-

ating software implements the new forecasting iteration. In case, if there is simultaneous failures of more than one computation module of AOBI&CS computation nod, the real time control software performs the implementation “shutdown” of those computational processes which occupy, corresponding to the number of failed computation modules, lower lines of the safety functions ranking table.

At introduction into the structure of an AOBI&CS CN the computation modules, which restored their operability, firstly there launched the application software of those safety functions, which were “shutdown” the last (in case if the flight configuration and/or the set of implementing AOBI&CS’s critical functions did not change). If the safety functions operating set undergo a change, only those computational processes are launched on the restored computation modules, which have a more higher position in the table of the aborted safety functions data-computing processes or should start the operation in the present time point. For this purpose the real time control software of the reconfiguration server, on the first lines of the corresponding table (displacing the other down), operatively table the information on which functional subsystems’ computational processes were aborted, and operatively delete those lines, which are relevant to the cancelled data-computing processes of those safety functions which implementation (activity) operating necessity is dismissed at aircraft flight configuration change.

Conclusions

The article describes the approach for assuring the specified (maximum possible) AOBI&CS’s functional safety level on the basis of using the reconfigurable computing subsystems computation node, which software is designed on hierarchical principle and allows to forecast the change of the Aircraft On-board I&C subsystems condition (reliability indexes and functional safety) to assure the reconfiguration implementation of its architectural-structural composition on different flight stages in case of unified computation modules failures.

The functional-architectural model of the corresponding AOBI&CS is proposed, which allows to evaluate the reliability and functional safety, considering the peculiarities of functional and architectural composition of the considered system, as well as to forecast the influence of software tools and hardware components failures on the safety of the whole system.

The method for assuring the specified or maximum possible AOBI&CS’s functional safety level on the flight operation stage is described, considering its real and forecasted condition, which takes into account the possible variants of AOBI&CS CN architectural-structural reconfiguration of computational resources in it.

The allocation of AOBI&CS CNs computational resources on the results of condition analysis on different operation stages is proposed for implementation using the updated in the real time mode ranging tables of active safety functions varieties of AOBI&CS, implemented on the corresponding operation stages, which consider the probability indexes of function operational failure, criticality levels of the computation modules, involved in its implementation, function importance weighting coefficient, which is defined at the design stage or by the aircraft crew (operator).

Notes:

- ¹ Viktoriya Pohyl, "The Enhanced Method of the Functional Safety of the Aircraft Onboard Information-Control Systems Analysis and Estimation," *Systems of Arms and Military Equipment*, vol. 2 (Kharkiv: Kharkiv Air Force University, 2010): 136-42.
- ² Ibid.
- ³ Viktoriya Pohyl and Aleksandr Kharybin, "The Estimation and Supporting Methods of the Functional Safety of the Aircraft Onboard control & Information System," *Radio-Electronic and Computer Systems* (2010): 278-82.
- ⁴ Aleksandr Kharybin, "About the approach to support the functional safety of the aircraft onboard information-control systems," *Systems of control, navigation and communication*, vol. 3 (Kiev: Central Scientific & Research Institute of Navigation & Control, 2010): 130-35.
- ⁵ Viktoriya Pohyl, "The Method to Support the Functional Safety of the Aircrafts Onboard Information-Control Systems on Their Operational Stage," *Systems of Arms and Military Equipment*, vol. 3 (Kharkiv: Kharkiv Air Force University, 2010): 68-74.
- ⁶ Viktoriya Pohyl, "The Enhanced Method and Informational Technology to Support the Functional Safety of the Aircrafts Onboard Information-Control Systems on Their Design Stage," *Science and Technology of the Air Force*, vol. 2 (Kharkiv: Kharkiv Air Force University, 2010): 65-70.
- ⁷ Pohyl, "The Method to Support the Functional Safety of the Aircrafts Onboard Information-Control Systems on Their Operational Stage."

ALEKSANDR KHARYBIN is Head of the Technical Analytics and Project Management Department of the Public Company Research & Production Corporation RADIY (Ukraine, Kirovograd), and focuses on the integration of information technology with reliability, survivability and functional safety. He graduated Poltava Military Telecommunication Institute in 2003 and received a PhD degree in Information Technologies from National Aerospace University named after Zhukovsky, Kharkov, in 2008. From June 2003 until March 2011, he was officer in service in the Ukrainian Armed Forces. Among other duties, he takes part in Ukrainian Armed Forces communication systems modernization and R&D programs in support of defence reforms.

VIKTORIYA POHYL is Lecturer of the Computer Engineering Department in the Poltava National Technical University named after Yuriy Kondratyuk (Ukraine, Poltava), and focuses on the integration of information technology with reliability and functional safety of the On-board Instrumentation and Control Systems. She graduated Poltava Military Telecommunication Institute in 2007.