IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# AN APPROACH TO THE DEVELOPMENT OF THE CONTROL SYSTEM OF THE AVIATION TRANSPORT SAFETY TAKING INTO ACCOUNT THE HUMAN FACTOR

**Alexander Rezchikov*, Olga Dolinina, Vadim Kushnikov, Vladimir Ivaschenko, Konstantin Kachur, Aleksey Bogomolov, Leonid Filimonyuk**

* Institute of precision mechanics and control of Russian Academy of Sciences, Russia
Yuri Gagarin State Technical University of Saratov

**DOI**: 10.5281/zenodo.290188

## ABSTRACT

In the paper the causes of accidents are considered as consequences of subsystems failures and personnel errors in air transport system. It has been shown that each such event is a systemic one and has a causal relationship with the other events and processes. There is proposed an approach for the classification of human factors in aviation and transport system based on the set-theoretic representation.

**KEYWORDS:** Air transportation system, emergency situation, human factor, safety.

## INTRODUCTION

Currently the task of maintaining security and preventing critical situations that arise during Air Transport Systems (ATS) functioning has become very important [1]. Despite the improvement of existing systems, the number of accidents, incidents and related risks have not been reduced. It should also be noted that completely secure systems  are not existed, and in fact nonhazardous human errors and equipment malfunctions that do not lead to accidents occur in all complex systems. As the experience of the aircraft exploitation shows, the role of the so-called "human factor" in the causes of air accidents is constantly increasing. "Human factor" is usually associated with events that are not covered by documentation, or become the result of non-fulfillment of actions prescribed by documentation. For aviation of the middle of the XX century the ratio of structural and design-and-manufacturing reasons (DMR) of catastrophes on the one hand and errors of the crew and flight support services on the other hand was about one to one. Currently, the ratio is considered to be about one to ten.

That is why the task of the development of the approaches to the analysis and prevention of emergency situations through a comprehensive study of the heterogeneous ATS functioning factors, including human-machine interaction is very important.

## THE HUMAN FACTOR IN ATS

The human factor (HF) is multifaceted and is associated with a variety of human roles in the system lifecycle including its conception and design, which should be taken into account during development of models and methods of ATS description, analysis and implementation. Results of the analysis [1] show that "human factor" determines flight safety (FS) and the aircraft's usage efficiency to large extent.

New aircraft's types are developed with previous generations' accumulated "sad" experience taken into consideration, however bringing them into service  does not guarantee the elimination of accidents, as new airplanes are provided with new systems designed to improve the efficiency of the transport exploitation. "Trial and error" method [1] has a limit for flight safety increasing. We estimate this limit as about 5 - 10 million flight hours of the same type aircraft's park for a single catastrophe.

A fundamentally new approach for the ATS security models creation is required to resolve this issue. The IL-86 reliability-safety model (RSM) was created during it designing. RSM model adequately reflects the reliability properties and safety of aircraft. This model is based on the concept of functional failure (FF). The term functional failure refers to inoperable state of the system as a whole, characterized by a specific violation of its functions independently of the condition causes. Functional failure of each system is determined through effects exerted on its functioning. It is characterized by the impact on other systems and on the airplane as a whole.

IL-86 aircraft's reliability-safety model allowed to establish all potentially possible FF, which can occur during operation. Each FF degree of danger is defined with the expected operating conditions taken into account. The design of systems is implemented in the way that all FF which can lead to an emergency situation (ES) or disaster situation (DS) are almost unbelievable, and there is no single failure causing the ES or DS. To mitigate the consequences of FF which can occur during the flight there are clear unambiguous recommendation to the crew. Following them guarantees the successful flight completion. All these recommendations have been tested in bench and flight tests and have passed the necessary certification.

Flight safety ensuring technology was developed for the aircraft's designing stage. Implementation of new technology guarantees the achievement of the FS required level since the beginning of the first aircraft operation. However, the creation of a fail-safe airplane is a single step on the way of achieving the required level of ATS security.

Increase of ATS safety requires all its units and their interactions to meet Novozhilov's principles [1], which were used in the fail-safe airplane designing. It should be noted that the flight-safety ensuring methodology applied to aircraft's creation can be extended to the rest of the ATS units and foremost on the crew. Note here that one of the principles of the aircraft's creation [1] emphasizes that each crew member can make a mistake, but single crew error should not lead to an emergency or catastrophe.

All so-called crew mistakes should be divided into two types: the first one is a gross deliberate violation of the requirements stipulated in the instructions for flight operations; the other part of the errors includes unintentional errors associated with incorrect estimation of suddenly encountered situations during flight and wrong decisions as a consequence. Based on the principle adopted above, ATS should be structured in the way that intentionally requirements violation would be disadvantageous or impossible and any willful violation would be recorded by means of objective control, so perpetrators of these violations knew that the appropriate punishment is inevitable. The second type of the errors can be eliminated or their severity (danger) can be reduced if the design of the aircraft and all ATS units considers human capabilities and the fact that the crew sometimes has to work at the limit of their physiological capacity, when the risk of an inadvertent error increases.

The term "error" doesn't fit entirely for unintentional errors, as it is associated with the appropriate sanctions. This part of mistakes is unintentional, and they occur as a result of the "man - machine" system imperfection. In this case it is necessary to design a "man - machine" system in the way that a single failure or single operator error does not create an emergency or catastrophe in all expected operating conditions of the airplane and crew. This goal can be achieved by solving of the set of the problems.

The first task is the definition of all possible violations in human-machine interaction (all potentially possible failures and mistakes are considered) [2, 3]. The second task is the assessment of the possible violations danger degree of human and machine interaction [4]. The third task is the "man - machine" system design creation in the way that single failures or errors do not lead to an accident.

## THE PROCESSES IN THE AIRTRANSPORT SYSTEMS. A FORMAL APPROACH TO THE CLASSIFICATION OF THE HUMAN FACTOR

Studies have shown that the numerical, logical, and character variables and constants, as well as equations and relations using them are not sufficient for the construction of the formal definitions of both general and many particular ATS operation processes. Due to the complexity of processes and ATS state space large dimension, the exact analytical description of them in the context of the mathematical model is not possible.

Cause-effect description of objects and structures provides more opportunities for modeling. An ATS operation can be described by six basic clustering process groups and all possible combinations of 1, 2, ..., 6, of them.

Basic ATS processes are the following:

$P_1$ – command, information and control processes;

$P_2$ – crew and air traffic controllers actions and training processes;

$P_3$ - units and ATS subsystem (primarily the aircraft) functioning processes;

$P_4$ – fuel and energy supplying processes for ATS (including airplane);
$P_5$ –supplying processes (cargo, meals, etc);
$P_6$ - processes of interaction with the environment: weather conditions, etc.

Depending on ATS decomposition level, dimension of the problem can be very high, even despite the finiteness of cluster processes set. However, this is not an unsolvable problem for ATS research, because the performance of computers has been steadily increasing and the authors have developed a cause-effect approach [5], as well as models, methods and algorithms to provide an acceptable dimension level.

Characteristics for the HF classification in the ATS can be represented by the following sets:

- *P* – by ATS process type according to [1]: taxiing, takeoff run, takeoff, ascending, en-route, descending, landing, etc.
- *C* – by type of crew and flight operators control processes of preliminary investigation of the flight situation from collecting of information for decision-making to the making decision.
- *H* – by time intervals: continuous tracking, for a minute, an hour, a day, etc.
- *L* – by the stages of the life cycle: design, manufacturing, operation and recycling.
- *S* – by the situation: regular, complicating the flight conditions, complex emergency, catastrophe.
- *Z* –by the consequences: positive (lead to the dangerous situation elimination) or negative (lead to the aggravation of the situation or accident).
- *E* – by environmental conditions: favorable, neutral or unfavorable.

Using ATS operation process deep detailing, HF circumstances in each case can be characterized by elements of the Cartesian product F:

$$F = C \times P \times H \times L \times S \times Z \times E.$$

Any "man-machine issue" can be classified and coded using *F*. For example, aircraft's landing task, as well as definitions and critical situations prevention, is identified as a subset in the following way:

$$\{C_1, C_2\}\times\{P_1, P_2, P_3, P_4\}\times\{H_1\}\times\{L_1\}\times\{S_1, S_2, S_3\}\times$$
$$\times\{Z_1, Z_2\}\times\{E_1, E_2\},$$

where $C_1$ –obtaining and analyzing instruments responses and the environment by the crew, $C_2$ –decision-making, $P_1$ –descending before landing, $P_2$ - runway alignment, $P_3$ - holding, $P_4$ –touching the runway and running, $H_1$-minutes, $L_1$ - operation, $S_1$ – regular conditions, $S_2$ – critical situation, $S_3$ – accidents, $Z_1$ – HF eliminated dangerous situation, $Z_2$ – HF aggravated dangerous situation, $E_1$ – favorable weather conditions, $E_2$ – unfavorable weather conditions.

## A COMPREHENSIVE RESOURCE AND THE OCCURRENCE OF ATS ACCIDENTS

The ATS operation is the interaction of disparate processes that use the integrated resources of different types. There are technology resources, power supply resources, human resources: crew and air traffic controllers, normative basis: International and country level aviation rules. Crew resource means its psychophysiological state at a given time, as well as its skills. Critical resource depletion leads to an incident or accident. These resource consumption processes are mutually influenced by each other. Therefore, a systematic approach to accidents causes study and to accidents prevention is needed in the future. The study of the problem shows that it is necessary to pay special attention during the analysis of the critical situations in the ATS to the fact that almost every accident is a consequence of the so-called "negative circumstances." That's why researchers always try to find if it is possible to prevent a catastrophe or to avoid it. The answer to this question depends on the resources, technology and energy supply, which allows *FF* mitigation in time, as well as the crew and air resources that perform or do not perform the necessary actions.

Let's provide definitions of the key concepts that are introduced in the proposed approach.

The subsystem resource is its ability to solve a specific task or to function in a predetermined manner over a certain period of time almost without fail if other subsystems operate regularly. Technical subsystem resource is determined by the state of its parts and the presence of a consumables stock. Crew resource as the ATS subsystem is determined by psychophysiological state of the crew members, their level of training, flight hours to the norm ratio, and a number of features related to interaction within the crew.

An ATS comprehensive resource is a set of resources of its sub-systems and components, which is expressed as a vector of key subsystems heterogeneous resources. The introduction of the integrated resource concept is explained by the need of more accurate estimation of ATS functioning safety conditions. The value of the ATS residual resource as the estimated mean time between failures, which is calculated for a specified period of time without regard for a number of processes, in particular - the process of human-computer interaction, as practice shows, is not sufficient in the calculation of flight safety conditions.

Subsystem failure is regarded as a consequence of its resources lack at any given time. Functional failure appears as a consequence of failure of one or more ATS subsystems.

According to Novozhilov principle [1] (a single failure of any subsystem must not lead to an emergency situation) can be interpreted as a requirement to fend off possible failure due to redundancy in the system, or due to functional redundancy other systems that may belong to other ATS subsystems.

Some failures do not directly affect the solution of the current problem, but it does not eliminate further negative consequences. Some failures are parried by technical means, crews or air traffic controllers. A number of failures, being combined with each other over a sufficiently long period of time form events sequence, which generally leads to an accident. As a prerequisite for accident prevention, consider the following principle: the denial of an important subsystem must be either prevented or parried.

Consider subsystem $a_1$. The condition for the prevention of accidents connected with $a_1$, is the availability of the resources necessary for subsystem $a_1$, and (in the case of its lack) the availability of resources from other subsystems, which can be used to parry failure of $a_1$.

As the cause of ATS subsystem failure authors consider the reaching of certain critical value by the resource, assuming that this subsystem must continue functioning. Let the denial of some subsystem a1 not being prevented, i.e. at time t the value of its resources were not sufficient for the further functioning and the following inequality held:

$$r_{a_1}(t) < \underline{r_{a_1}} \,,$$

where $\underline{r_{a_1}}$ – certain critical resource value. Sign «<» may imply a numerical inequality, as well as the fact that $\underline{r_{a_1}}$ is not a subset of $r_{a_1}(t)$. Usage in this sense is relevant if there is a set of instructions represented by documents or stored into database and considered as a resource necessary for management.

Consider the case of failure in aircraft's subsystem $a_1$. In this case, there must be a possibility of failure parrying by resources of any other subsystems: $a_2$, $a_3$, …, $a_n$. If this is not possible, i.e. resources of these subsystems are not enough for parrying and the condition

$$(r_{a_2}(t) < \underline{r_{a_2}}) \wedge (r_{a_3}(t) < \underline{r_{a_3}}) \wedge \ldots \wedge (r_{a_n}(t) < \underline{r_{a_n}})$$

has "true" value, then "unfavorable circumstances" occur, which is formally means that the following expression holds

$$(r_{a_1}(t) < \underline{r_{a_1}}) \wedge (r_{a_2}(t) < \underline{r_{a_2}}) \wedge \ldots \wedge (r_{a_n}(t) < \underline{r_{a_n}}), \qquad (1)$$

where $\underline{r_{a_i}}$ – the critical values of operation parameters of the corresponding subsystems.

The condition fulfillment defines limits for emergency situation occurrence. Accordingly, a situation when $a_1$ subsystem operates properly or technical capabilities of subsystems $a_2$, …, $a_n$ allows to parry $a_1$ failure could be described as the negation of the condition (1)

$$(r_{a_1}(t) \geq \underline{r_{a_1}}) \vee (r_{a_2}(t) \geq \underline{r_{a_2}}) \vee \ldots \vee (r_{a_n}(t) \geq \underline{r_{a_n}}) \qquad (2)$$

If the condition (2) is met, the failure sequence is broken.
In general, the resources that appear in conditions (1), (2) may have different dimensions and different nature, which corresponds to a wide range of different ATS units.

Parrying of some subsystem failure is possible due to other subsystems functionality. The most important particular process that is always relevant for the ATS is a man-machine process with interaction performed between human functional and psychological capabilities and the technology functional capabilities, and the process of human-machine interaction. The latter includes components that provide operation convenience, ergonomics, the appropriate interface, the operator experience of work in a particular place by alone as well as together with another operator.

In general, there is a group of conditions for each ATS unit, each of which describes the set of adverse circumstances associated with this link. These conditions are formed on the basis of expert meetings, accident investigations, theoretical calculations and tests on simulators. Generally these conditions should include different time moments, according to the dynamics of some events flow. A sufficient condition for avoiding situations that are characterized by (1), is the timely resumption of ATS units functionality.

## AN EXAMPLE

As an example, consider the catastrophe of A310 airplane in the airport of Irkutsk, Russia. It happened in the summer of 2006, on the run landing stage. After rolling out of the runway, airplane collided with artificial obstacles and ignited. Fire killed 125 people, airplane's construction and components of its system suffered multiple destruction and partial destruction by fire. According to the official report [6], there has been the case of a number of adverse factors effects. Moving out of the runway is explained by crew uncontrolled actions on the run landing stage. This means the lack of crew resources at the particular moment:

$$r_{c_1}(t_1) < \underline{r_{c_1}}. \tag{3}$$

The lack of crew resources can be explained by stress, lack of knowledge, more than the norm fatigue, and consequently, a performance decrease .
Condition (3) appeared together with the fact that one engine reverse thrust was deactivated at the same time:

$$r_{e_1}(t_2) < \underline{r_{e_1}}, \tag{4}$$

which led to a set of run speed over 180 kph. High speed means little time for reaction which is given to the crew to prevent an accident. Parrying of functional failure did not happen, which implied crew resources lack, or the fact that the time to parry was significantly lower than the norm, and the crew could not parry the functional failure. Thus, there is a disjunction

$$r_{e_1}(t_2) < \underline{r_{e_1}} \vee r_{c_1}(t_3) < \underline{r_{c_1}} \tag{5}$$

as one of the adverse circumstances. In addition, there has been rolling out of the runway due to the uneven engines thrust, which means a lack of resources for their synchronization. The condition is: $r_{e_1}(t_4) < \underline{r_{e_1}}$.

Combining the conditions (3), (4) and (5), we find that the cause of the accident can be characterized by the following condition:

$$\begin{gathered} r_{c_1}(t_1) < \underline{r_{c_1}} \wedge r_{e_1}(t_2) < \underline{r_{e_1}} \wedge \\ \wedge (r_{e_1}(t_2) < \underline{r_{e_1}} \vee r_{c_1}(t_3) < \underline{r_{c_1}}), \end{gathered} \tag{6}$$

which is more complex than the expression of the form (1) that describes the inability to parry one FF by use of other sub-systems and their resources. Furthermore, in the expression (6) faults (3) - (5) of the various airplane's subsystems during figuring out details of further accidents can also be represented as a totality of several subsystems FF after clarifying of further accident details.

It should be noted that the resources that appear in these entry threat conditions, have different nature, including the human factor associated with dangerous involuntary actions of the crew. Application of the above body allows analyzing the position of incident or accident in the ATS using systematic approach. Proposed logical conditions allow us to describe the incident and resource values, the lack of which leads to accidents.

## CONCLUSION

The study proposes approaches to the description of functioning and development processes of aviation transport system based on the use of cause-effect system for ATS operation, which includes interaction among a large number of heterogeneous processes, including the operation of equipment and human actions.
It is proposed to use the further improvements of the research results in the following areas:

– in the process of specialists training in the relevant areas;

– in the development and improvement of training simulators for the ATS personnel (pilots, air traffic controllers);

– in the developing of aviation and transport systems' subsystems and components.

– as a tool for systematization and formalization of the accidents circumstances description, using it for their investigation, as well as for prediction of possible emergency situations in the ATS.

The results of the research can be used in the ATS security ensuring and maintaining system across the state or industry. In this context, for essential increase of the ATS security level in Russia the following is required:

– to create a model of reliability and safety of all ATS units as a whole;

– to develop technology-based requirements for fail-safety, including operator errors for the ATS as a whole and its units, on the basis of created reliability and security models;

– to improve the existing ATS and its units on the basis of flight safety requirements and applying to the "human - machine" system the same principles that have been described for the material part of the airplane;

– to create a methodology for assessing the conformity of each unit and AST in general to fail-safe requirements, taking into account operator error;

– to organize ATS and all its units on the basis of common principles and requirements to ensure the safety of flight;

– to issue licenses for the airplane operation considering implementation of the previous two paragraphs;

– to create a united aviation safety information system of Russia.

## ACKNOWLEDGEMENT

The research is supported by Russian foundation for Fundamental Research, grant number 16-01-00536 a.

## REFERENCES

[1] G.V. Novozhilov, M.S. Neymark, L.G. Tsesarsky, “Safety of the flight of an airplane: Conception and technology,” in: *Publishing house of Moscow Aviation Institute*, 2007.

[2] V.A. Tverdokhlebov, “Geometrical approach to technical diagnosing of automatons,” in *Proc. of IEEE East-West Design & Test Symposium*, Sevastopol, 2011, pp. 240-243.

[3] A.S. Epifanov, “Recognition of automatons by their geometrical images,” in *Proc. of IEEE East-West Design & Test Symposium*, Sevastopol, 2011, pp. 381-384.

[4] A. Rezchikov, V. Kushnikov, V. Ivaschenko, A. Bogomolov, L. Filimonyuk, K. Kachur, “Control of the air transportation system with flight safety as the criterion” *Automation control theory perspectives in intelligent systems*, vol. 466, pp. 423-432, April 2016.

[5] L.Yu. Filimonyuk, **“**Cause-effect model of aviation transport system's functioning,” in *Critical Infrastructure Safety and Security: Proceedings of the First International Workshop*, vol. 1, Kirovograd, 2011, pp. 164-167.

[6] An account about results of investigation of aviation accident. Catastrophe of Airbus A-310. *An account of International aviation committee*. [Online]. Available: www.mak.ru/russian/investigations/2006/A310_09-07-2006.pdf