Mathematical foundation of system design regulatory controls based on ARP4754A

Vladimir Kulabukhov
Moscow research and production complex "Avionika" named after O.V. Uspenskiy, 7 Obraztsova, Moscow 127055, Russia

kws0704@mail.ru

Abstract. The article provides an interpretation and formal mathematical foundation in the language of modern algebra for V-process of designing complex systems recommended by the ARP4754A manual, in the context of a new paradigm in mathematical systems theory developed on the basis of the General principle of isomorphism. This provides a scientific basis for the widely used design approach

1. Introduction
The design problems of modern technical systems are often related to the fact that many of these systems are complex. For complex systems, it is impossible to construct a deterministic model that characterizes the one-to-one relationship between inputs and outputs [1]. Existing models do not allow us to accurately predict the behavior of the system in all possible situations. At the same time, many of the designed systems are critical for their intended purpose to ensure the safety of the operation of the corresponding objects in operating modes. Such systems are called systems with full responsibility. When designing systems with full responsibility, the risks of accidents and catastrophic events should be minimized — such events should become almost impossible. This is especially true for systems related to aviation.

In the absence of deterministic models to ensure a given level of reliability, complex aviation systems must be tested for safety in all possible flight situations under the expected operating conditions after development. However, the complexity of the systems does not allow, firstly, even to anticipate all possible flight situations and, secondly, to perform a very large amount of test work even for obvious situations. In addition to the cost of testing, the time frame for completing tests is also important, which can be very long. The question arises: how to resolve the contradiction between the immensity of the volume, cost and timing of tests on the one hand and ensuring a given level of reliability of equipment and flight safety, on the other hand.

The solution to this contradiction in the design of complex systems was found not in certifying an already developed, ready — made and tested system, but in extending the certification and quality control procedure to the entire development process from the very beginning—the moment when the requirements for the system and the technical task for its development were formed. In this case, not only the design procedures are subject to verification, but also the qualifications of the personnel involved in their implementation, as well as the structure and level of equipment of the design organization with the necessary equipment and software. In fact, it is assumed that high-quality design
procedures performed by qualified personnel under proven conditions guarantee the high quality and reliability of the developed system.

For complex systems, this approach is considered rational. It was tested in practice, proved to be in demand and was fixed in the regulatory documents regulating the procedures for designing and certifying complex systems. One of the main and system-forming in this area is the guide to the development of civil aircraft and systems ARP4754A [2]. The document refers to the full cycle of design and manufacture of aircraft and other complex aircraft systems and recommends using the V-model of the design process and its verification, shown in figure 1 [2].

![Figure 1. V-model of the aviation engineering design process.](image)

The ARP4754A manual addresses the processes of functional safety and aircraft design in the General context of certification. The approach recommended in the guide is essentially a heuristic approach. However, after discussion by the expert community, testing in practice and acceptance for practical guidance by the majority of developers and certifying bodies, the approach has acquired a very high level of objectivity. To date, ARP4754A has been widely recognized and is actually used as a standard for the development and certification of complex aviation systems. The ARP4754A manual is a Central element in the system of documents that govern the full development cycle of the aircraft and its complex systems that are critical to flight safety.

The design approach recommended in ARP4754A is widely used in design practice, developed and discussed in the literature [3–12]. However, questions remain about its scientific validity. This article considers one of the possible variants of such justification in the language of modern mathematics.

In [13, 14], a goal-oriented approach to system design is considered and justified. This approach is similar in many ways to the design approach recommended by ARP4754A: both approaches suggest using a top-down design procedure - from General requirements to specific requirements and further to hardware and software development, to their integration in local devices and in the system as a whole. The difference is that the goal-oriented approach from the very beginning provides for the decomposition of the structure of the designed system into a strictly defined set of independent but interrelated architectures [13, 14]. The interconnection of architectures is determined by the goal of designing a single system that corresponds to a strictly defined purpose, that is, providing for the implementation of specified functions. The sequence of architecture development and their subsequent integration into the system structure as a whole is formalized and prescribed. The approach recommended by ARP4754A does not focus on the structure and architectures of the system – they are chosen by the developer at his discretion, but so that all the requirements and functions prescribed for the system are carefully analyzed and detailed, and then these functions and requirements are implemented both in the local hardware and in the system as a whole. In contrast to the design procedure recommended by ARP4754A, the goal-oriented approach has a fairly strict mathematical justification [14] based on the General principle of isomorphism [1, 15], which is successfully applied
to solving various problems in algebraic systems theory [14–17]. We investigate the possibility of applying the General isomorphism principle to formalize the approach to designing complex systems, discussed in the document ARP4754A.

2. Description of the research

Even a brief comparative analysis of the goal-oriented approach [13, 14] and the $V$-process design approach [2] recommended by ARP4754A shows that the $V$-process can also be interpreted and convincingly justified in terms of the General principle of isomorphism in system theory.

In [14] it is shown that from the point of view of mathematics the approaches to top-down design from goals to resources and bottom-up design from resources to goals are equivalent, because there must be a one-to-one correspondence between the objectives (requirements) and resources, based on which the system is implemented. This one-to-one correspondence, from the viewpoint of mathematics, is called isomorphism. The structure of the system is a form of manifestation of this isomorphic mapping of system goals and requirements into resources and, conversely, resources into goals. However, for a number of quality criteria and indicators, such as the level of integration of resources, efficiency and cost of their use in the system structure, it is more preferable to design "top-down" from the goals (requirements) to resources. This design simplifies the formation of the structure itself and its constituent architectures [13, 14]. The formalization of a purposeful approach to system design in the language of algebra is given in [14]. However, the formalization in the language of algebra of the design approach using the $V$-model recommended by ARP4754A will be somewhat different. Let’s explain this.

The main result of a new paradigm in algebraic systems theory based on the General principle of isomorphism is the theorem on the realization of isomorphism by a composition of maps [1, 15]. Based on Figure 2, we present here a statement of the theorem without proof.

![Figure 2. Commutative diagram of the mappings for of the theorem on the realization.](image)

The theorem on the realization: if there is a model $f : X \rightarrow Y$ that maps data $X$ to data $Y$ isomorphically and there are mappings $g : X \rightarrow Z$ and $h : Z \rightarrow Y$ such that the composition $f = hg$ holds, then

- a) up to the model-isomorphism $f$, the data $X$ and $Y$ are accurate and complete;
- b) the model $f$ is minimal and unique in the sense that if there is another model-an isomorphism $f^* : X \rightarrow Y$ that explains the same data, then there is also a unique isomorphic map $\varphi : f^* \rightarrow f$ such that the relations $f = \varphi f^*$ and $f^* = \varphi^{-1} f$ are satisfied, that is, the maps $f$ and $f^*$ are isomorphic to each other: $f \cong f^*$.
- c) the maps $h$ and $g$ in the composition $f = hg$ are isomorphism maps up to the isomorphism of $f$.

The proof of the theorem is given in [1], and the rules and examples of determining inverses for maps appearing in the commutative diagram in Figure 2 are illustrated in [15]. The theorem on the realization essentially repeats the formulation of the General isomorphism principle given in [1]. The main mathematical result contained in the theorem on the realization is that the maps $h$ and $g$ that are not isomorphic separately, outside the commutative diagram, have all the properties of isomorphic maps inside the commutative diagram, that is, they have in this commutative diagram the only inverses $h^{-1}$ and $g^{-1}$ and are thus isomorphisms up to the unconditional isomorphism $f$. The map $f$ is inherently isomorphic even outside the commutative diagram and is therefore called an unconditional isomorphism. The composition $f = hg$ may not be unique: there may be another composition
\( f = h'g' \) of other maps of \( h' \) and \( g' \) that implements the same isomorphism \( f \). The mappings \( h' \) and \( g' \) will also satisfy all the conditions of the realization theorem, and these mappings will have their own unique inverse mappings \( (h')^{-1} \) and \( (g')^{-1} \) inside the corresponding commutative diagram.

From the point of view of our research, it doesn't matter what algebraic structures are meant when we talk about "data" \( X \) and \( Y \) in Figure 2. It is important that the map \( f \) "recalculates" elements and rules for working with them from the algebraic structure \( X \) to elements and rules for working with them in the algebraic structure \( Y \). In terms of this work, "data" \( X \) will mean the set of goals of the system (requirements for it) and the relationships between them, for example, the relationship of coordination and subordination (subordination) of requirements and goals. "Data" \( Y \) refers to the set of resources (software, hardware, and others) and the relationships between them that are used to achieve these goals. As examples of relationships on a set of resources, you can specify the relationships of nesting resources and relationships between homogeneous resources (for example, hardware and functional modules are embedded in crates, and crates are combined by link lines in a redundant integrated system). By "data" \( Z \) we mean some algebraic structure that characterizes the embedding of a set of goals-requirements \( X \) in a set of local resources \( Z \) and the rules for working with "local embeddings" in the algebraic structure of \( Z \). Then the mapping \( g \) characterizes the procedure for decomposing global goals \( X \) (goals-requirements of the highest level) into local goals, that is, building a tree of goals, as well as rules for embedding them in local resources. The mapping \( h \) interprets the procedure for integrating (combining) local resources \( Z \), with local goals nested in them, into a common set of global resources (top-level resources) \( Y \) that implement system goals as a whole (top-level goals).

Taking into account the mathematical formalism of the theorem on the realization and its meaningful interpretation in terms of our work, the \( V \)-process of designing and certifying complex systems recommended by the ARP4754A manual can be displayed as nested commutative diagrams shown in figure 3.

![Figure 3. Commutative diagram for the V-process.](image)

Figure 3, as well as figure 1, shows how subsets of lower-level local goals \( X_1...X_N \) are formed on the descending branch of the \( V \)-process from the initial set of top-level goals \( X \)-requirements, taking into account the provision of end-to-end traceability of goals on the "top-down" principle. This eliminates the loss of goals, besides, the use of the local mappings \( g_1...g_N \) provides implementation of each goal in some "own" local resource \( Z_1...Z_N \). On the ascending branch of the \( V \)-process, local subsets of resources \( Z_1...Z_N \) with particular goals implemented in them are integrated into resources of higher and higher levels \( Y_1...Y_N \) by means of unifying mappings \( h_1...h_N \). At the same time, each level of consideration of the "goals — resources" mapping must provide its own local isomorphism \( f_1...f_N \).
between goals \( X_1...X_N \) and resources \( Y_1...Y_N \) of the corresponding level, up to goals-requirements \( X \) and resources \( Y \) of the highest, system level.

The ARP4754A manual does not describe the actual procedure for decomposing goals-requirements, i.e. it does not contain a procedure for generating local mappings \( g_1...g_N \), but it imposes restrictions on the quality of these procedures, provides traceability of goals and requirements when moving to local levels, and contains criteria for evaluating the quality of decomposition. The same applies to procedures \( h_1...h_N \) integration of local resources into the General procedure \( h \) for creating system resources \( Y \) that meet the goals \( X \) of creating the system as a whole. The ARP4754A manual requires that at each level of the system review, the composition of local maps \( h_i \) and \( g_i \) gives a local isomorphism \( f_i = h_i g_i \), that is \( i = 1...N \), and provides a one-to-one correspondence between the goals-requirements and resources of the corresponding level.

In addition, one of the main tasks solved by the document ARP4754A in relation to the system design process is the implementation of the superposition principle, which is a consequence of the implementation theorem and the General isomorphism principle [1]. The essence of the superposition principle in the context of this article is that a superposition or, in other words, a certain "sum" (summation will be denoted by a sign \( \oplus \) ) of maps \( g_1...g_N \) gave the total mapping \( g = g_1 \oplus g_2 \oplus ... \oplus g_N \). "Sum" of mappings \( h_1...h_N \) gave a General mapping \( h = h_1 \oplus h_2 \oplus ... \oplus h_N \). The "sum" of mapping-isomorphisms \( f_1...f_N \) gave a General isomorphism \( f = f_1 \oplus f_2 \oplus ... \oplus f_N \) between the goals-requirements \( X \) and resources \( Y \) of the System as a whole.

The implementation of the isomorphism \( f \), that is, the creation of a complex system (an aircraft or an aviation system as a whole) cannot be carried out directly and instantly. The isomorphism \( f \) can only be realized through the implementation of the design process, that is, through the implementation in the form of a composition of processes-maps \( h \) and \( g \), such that \( f = hg \). This is the meaning of both the implementation theorem and the General principle of isomorphism [1, 15], and the recommended document ARP4754A \( V \)-process for designing complex systems. By the theorem on the realization, the maps \( h \) and \( g \) have the only inverses \( h^{-1} \) and \( g^{-1} \) in the commutative diagram in figure 3. This means that you can also check the design quality of a complex system in reverse order: from system resources \( Y \) to local resources \( Z \) (with local goals implemented in them) and then to system goals-requirements \( X \). If another design organization implements an isomorphism \( f \) between the goals and resources of the system using the composition \( f = h'g' \) of other maps \( h' \) and \( g' \), then these maps will also have to meet the requirements of the theorem on the realization and the \( V \)-design model recommended by ARP4754A.

Thus, it is shown that the \( V \)-design process of complex systems, guideline ARP4754A as a deliberate design approach [13, 14], has not only clear the meaning and rationale, but it also allows for a convenient and strictly formalized description in the language of modern algebra and rationale from the point of view of the General principle of isomorphism in mathematical systems theory. This provides a scientific, formal mathematical foundation for the widely used design approach recommended by the ARP4754A document, which ensures the validity of its use in the future.

References
[1] Kulabukhov V S 2018 The General principle of isomorphism in systems theory Cloud of Science 5(3) 400–72
[2] Guidelines for Development of Civil Aircraft and Systems 2010 ARP 4754A US SAE International: Warrendale, PA, USA, 21 December 2010
[3] Noviello M C, Dimino I, Concilio A, Amoroso F and Pecora R 2019 Aeroelastic assessments and functional hazard analysis of a regional aircraft equipped with morphing winglets Aerospace 6 (10) 104 doi: 10.3390/aerospace6100104
[4] LI Xiaoxuna, Zhu Yuanzhenb, Fan Yichenb, Su Duoa 2011 A Comparison of SAE ARP 4754A
and ARP 4754. *The 2nd International Symposium on Aircraft Airworthiness (ISAA 2011) Procedia Engineering* **17** p 400 doi: 10.1016/j.proeng.2011.10.047

[5] Esdras G and Liscouët-Hanke S. 2015 Development of Core Functions for Aircraft Conceptual Design: Methodology and Results *Canadian Aeronautics and Space Institute AERO 2015 Conf.* https://www.researchgate.net/publication/277021129

[6] Mathew PG 2019 Model-Based System Engineering Methodology for Implementing Networked Aircraft Control System on Integrated Modular Avionics — Environmental Control System Case Study https://spectrum.library.concordia.ca/985095/7/GeorgeMathew_MASc_S2019.pdf

[7] *A publication of the International Council on Systems Engineering* December 2019 **22** 4 http://www.panetto.fr/INSIGHT_vol-22-issue-4.pdf

[8] Schulze J 2018 *Architectural Design of a Future Flight Management System Supporting 4D Trajectories. Dissertation* D17. Darmstadt 2018 https://tuprints.ulb.tu-darmstadt.de/8386/1/DissertationSchulze.pdf

[9] Altfeld H H 2010 *Commercial Aircraft Projects: Managing the Development of Highly Complex Products* (Farnham)

[10] *Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments* ARTEMIS Call 2013 project 621429 https://www.artemis-emc2.eu/fileadmin/user_upload/Publications/Deliverables/EMC2_D6.1_SotA_for_System_Qualification_and_Certification_final.pdf

[11] https://afuzion.com/arp4754a-introduction-avionics-systems/

[12] *Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes—CS-25, Amendment 11* 2011 European Aviation Safety Agency: Cologne, Germany

[13] Kulabukhov V S 2015 *Aviakosmicheskoye priborostroyeniye* **12**:11–31

[14] Kulabukhov V 2019 Algebraic Formalization of System Design Based on a Purposeful Approach *IOP Conf. Series: Materials Science and Engineering* **476** 012017 doi: 10.1088/1757-899X/476/1/012017

[15] Kulabukhov V S 2019 A General Principle of Isomorphism: Determining Inverses *Symmetry* **11** 1301 doi:10.3390/sym11101301

[16] Kulabukhov V S 2018 *IOP Conference Series: Materials Science and Engineering* **312** 012016 https://doi.org/10.1088/1757-899X/312/1/012016

[17] Kulabukhov V 2017 *MATEC Web of Conf.* **99** 03008 doi: 10.1051/matecconf/20179903008