Сборник докладов 1-ой франко-российской конференции "Модели долговечности, старения и деградации в теории надежности, медицине и биологии", 7-9 июня 2004 г., С-Пб., С. 42-51

# Analytical-Tabular Calculation Method of Reliability Measures and its Application in Process of Estimating Failure-Free Operation of Metro Safety Systems

Y. V. ANTONOV, V. P. BELOV, A. D. GOLYAKOV, S. J. STARKOV

"Research Institute of Fine Mechanics" Joint-stock company,
Russia, St.-Petersburg, E-mail: Golyakov@niitm.spb.ru

An analytical-tabular calculation method of reliability for bus-structured information control systems is considered, for illustration, in the process of estimation of failure-free operation measures of safety systems for the St.-Petersburg Metro train traffic. This method can be used in the process of predicting and creating reliability models of complex diagnostic and information systems for medicine and safety systems for thermal and nuclear power engineering.

The present phase of developing science and engineering is characterized, on the one hand, by growth of complexity of manufactured products, and on the other hand, by rigid requirements imposed for their reliability. Despite sufficiently vast experience stored in our country and abroad and significant results achieved in the field of theories of design and tests of complex information control systems, a number of unsettled problems remain in the sphere of estimation methodology of reliability measures at early stages of product life cycle.

These problems arise especially urgent in the process of developing control systems of objects considered the most dangerous. Such systems are dangerous not only for dependent objects and service personnel but also for population and environment. Therefore reliability occupies one of the central places among the properties constituting a notion of quality of such control systems.

Modern electronic components used in promising control systems have a mean operating time to failure of several hundred thousand hours up to several million hours.

The complex systems comprising these components, in their turn, have a really achievable operating time to failure of 50-100 thousand hours, which does not meet the present-day requirements for duration of their operation.

Moreover, the systems in which the failure of a separate element can prove "dangerous" have particular significance. Under certain conditions such a failure, which is a source of safety threat, can cause either human victims and traumata or grave economic, ecological and other undesirable consequences, for example, loss of enterprise-developer authority or decrease in consumer demand for output production.

Experience stored in the "Research Institute of Fine Mechanics" Joint-stock company ("NII TM" JSC) in the field of development, manufacture and operation of science-intensive control systems shows that effective ways of counteracting dangerous failures are the following:

- application of electronic circuits and components with large-scale and very large-scale integration;
- maintenance of lightened modes of operation of the electronic circuits and components;
- development of methods of assembling, testing and operating apparatus;
- use of majority circuits based on principle "two out of three", "three out of four" etc., and also application of circuits including safe terminals or else circuits "by asymmetrical failures."

By circuits "by asymmetrical failures" the circuits proper and their physical components switching a system to safe ("protective") state by means of generating appropriate control signal in the event of any single internal damage or interruption are understood.

Now, for example, let us imagine an hierarchical control system consisting of two or three levels at a level of functional units. It is assumed that each level of the system is provided with input and output two-out-of-three majority circuits and duplicated circuits "by asymmetrical failures" for receiving and outputting signals and commands for controlling executive devices. It is supposed that, in addition, the system is equipped with several workstations and a certain maintenance program and that a subsystem for monitoring, diagnosing and disabling (recovering) damaged components is applied to the system as a whole. In the present case a question of reliability measures calculation methodology and calculation proper no longer arises – it is obvious that this problem is extremely difficult.

Scientists and specialists of reliability service of the "NII TM" JSC encountered this problem at the end of the 1980s when they were charged with developing an explosion and fire prevention system for "Energiya-Buran" complex. This system containing on-board and ground apparatus assured safety of pre-starting procedure, launch and flight of the carrier rocket. The system comprised the following devices:

- three channel on-board computer;
- specialized microprocessors connected on majority principle;
- supply and amplifier units under redundancy, etc.

The necessity of developing new approaches to estimation methodology of reliability measures for complex information control systems became especially urgent in the process of developing an integrated safety and automated control system for Metro train traffic ("Dvizheniye" system). This system forms an hierarchical structure and incorporates into a single whole hardware and software for controlling objects of three different levels.

The uppermost level of "Dvizheniye" system is a Metro line central dispatcher post (CDP). The second hierarchical level of the integrated control system for Metro train traffic is a station level. This level consists of the following components:

-stationary apparatus (SA) of stations and stages;

- hardware and software for ensuring microprocessor-based Metro interlocking (MMI); and

- communication channels for connection with train-borne apparatus (TA) and SA of adjacent stations. The third hierarchical level (train level) includes equipment and facilities for controlling Metro train traffic.

Apparatus of all three levels are linked in a single whole by using the four main subsystems (see Fig.1), which are the following:

- train traffic safety subsystem;
- train traffic control subsystem;
- information subsystem;
- subsystem for monitoring and diagnostics.

A group of analytical methods of calculating reliability measures at early stages of information control system life cycle has been devised as a part of the theory of reliability. These methods have shown a good performance, and now they are widely used in practice. The methods of this group are the following:

- structural-analytical method;
- logical-graphic methods;
- logical-probabilistic methods;
- analytical-statistical methods, etc.

Selection of the calculation method is made on the basis of analysis of information control system structure, degree of labour intensity of estimation process, experience and qualification of performers, availability of resources and required information for performing calculation, and other factors.

Performed analysis of the structure of "Dvizheniye" system, which includes three channel information bus under redundancy, two channel control bus under redundancy, power supplies under redundancy, and units provided with three channel inputs and two channel outputs, has shown that reliability measures calculations made on the basis of the above methods are an extremely difficult and labour-intensive process. In this connection, an estimation method of reliability of power supplies under redundancy, functional units under internal input and output redundancy, and bus-structured systems has been devised.

The method devised is founded on the approach based on tables of decisions (truth tables), which has been suggested by E. G. Henley and J. Kumamoto H. in the monograph "Reliability of technical systems and estimation of risk" [1]. Therefore this method is known under the name "an analytical-tabular method."

The tables of decisions are submitted in this well-known monograph for two versions of elementary functional unit. One of them consists of two elements under loaded redundancy, and another comprises two-out-of-three majority circuits. In future the tables obtained are made use of in the purpose of determining minimal unsafe combinations of technical states of units included in system.

The essence of the method examined in the present report consists in distribution of functional units of an information control system (ICS) into several hierarchical levels. The number of the levels is established depending on complexity of the system under consideration.

Units equipped with information buses connected to systems, which are external in respect to the system in question, relate to the first level. For example, this level can include secondary power supplies switched on in response to commands from external control systems. Besides, this level comprises units without information (input) buses, for example, primary power supplies, measuring devices provided with their own sources of energy for determination of environmental parameters, etc.

The second hierarchical level consists of functional units equipped with information and power buses connected to control (output) buses from the first level.

The third and the following levels of the proposed hierarchical structure contain units, information inputs of which are connected to control buses from functional units of the lower levels. A calculation sequence in accordance with the analytical-tabular method consists of the following steps.

1. A list of up states (states of operability $(S_w)$) of all functional units of the system is made ($w = \overline{1,\Omega}$, where $\Omega$ is for the number of units in the system), and probabilities of these states are calculated on the basis of known values of failure-free operation probabilities (reliability functions) of channels under redundancy.

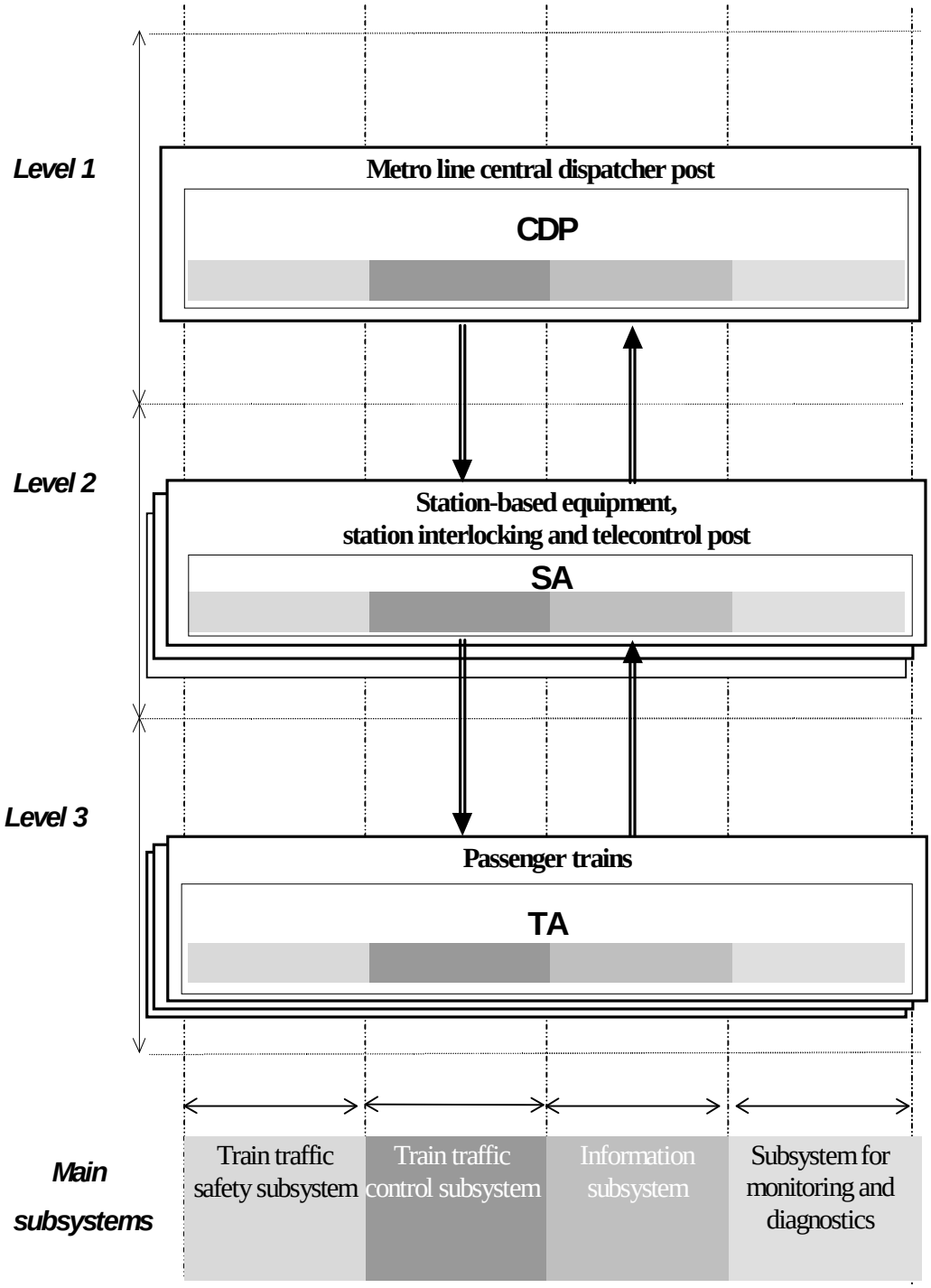


Fig.1. Hierarchical levels of the integrated safety and automated control system for Metro train traffic and the main subsystems.

For example, required probabilities for a three-channel power supply unit are determined in accordance with the following formulae:

$$\begin{gathered} P(S^{111}) = p_k^3, \\ P(S^{110}) = P(S^{101}) = P(S^{011}) = p_k^2(1-p_k), \\ P(S^{100}) = P(S^{010}) = P(S^{001}) = p_k(1-p_k)^2, \end{gathered} \tag{1}$$

where $S^{111}$ is the unit state, at which all three channels are in up state;

$S^{110}, S^{101}, S^{011}$ are the unit states, at which one of the channels is in down state (state of non-operability), and the other two are in up state;

$S^{100}$, $S^{010}$, $S^{001}$ are the unit states, at which two channels are in down state, and one channel is in up state;

$p_k$ is probability of failure-free operation of one channel of the unit.

2. The units of the first hierarchical level are selected. It is obvious that probabilities of up states ($W$) of output buses of these units are equal to probabilities of appropriate up states calculated at the first stage, i. e.

$$P(W) = P(S). \quad (2)$$

3.The second hierarchical level consisted of the functional units, for which matrices of technical states are drawn up, is formed.

Each functional unit of this level consists of a collection of interconnected elements. A mathematical model of reliability of a unit provided with information, control and power buses under redundancy is represented, as follows:

$$M = \{Y, Z, S, W, F\}, \quad (3)$$

where Y is a set of states of the unit information buses, and it is represented, as follows:

$$Y = \{Y^V\}, \ V = \{V_1, V_2, ..., V_j\};$$

$j$ is the number of the unit information buses under redundancy;

$Z$ is a set of states of the unit power buses, and it is determined, as follows:

$$Z = \{Z^x\}, \ x = \{x_1, x_2, ..., x_y\};$$

$y$ is the number of the unit power buses under redundancy;

$S$ is a set of the unit technical (internal) states, and it is expressed, as follows:

$$S = \{S^V\};$$

$W$ is a set of states of the unit output (control) buses, and it is determined, as follows:

$$W = \{W^z\}, \ z = \{z_1, z_2, ..., z_n\};$$

$n$ is the number of the unit output (control) buses;

F designates mapping of a set $[Y \times Z] \times S$ into the set W, i.e.

$$[Y \times Z] \times S \xrightarrow{F} W.$$

Top indices of the sets Y, Z and W are given as alphabet [0, 1]. The set index value equal to zero corresponds to down state of the bus, and the index value equal to unit corresponds to up state. A state matrix realizing the mapping F is compared to the mathematical model (3). The state matrix is given as table. For example, a unit comprising two information inputs, two power buses under redundancy, and a single control output corresponds to the matrix represented by Table1.

Table 1. State matrix

| Y | Z | S | | |
|---|---|---|---|---|
| | | $S^{11}$ | $S^{10}$ | $S^{01}$ |
| $Y^{11}$ | $Z^{11}$ | $W_1^1$ | $W_8^1$ | $W_{12}^1$ |
| | $Z^{10}$ | $W_2^1$ | $W_9^1$ | $W^0$ |
| | $Z^{01}$ | $W_3^1$ | $W^0$ | $W_{13}^1$ |
| $Y^{10}$ | $Z^{11}$ | $W_4^1$ | $W_{10}^1$ | $W^0$ |
| | $Z^{10}$ | $W_5^1$ | $W_{11}^1$ | $W^0$ |
| | $Z^{01}$ | $W^0$ | $W^0$ | $W^0$ |
| $Y^{01}$ | $Z^{11}$ | $W_6^1$ | $W^0$ | $W_{14}^1$ |
| | $Z^{10}$ | $W^0$ | $W^0$ | $W^0$ |
| | $Z^{01}$ | $W_7^1$ | $W^0$ | $W_{15}^1$ |

The lines and columns containing states ($Y^{00}$ and $Z^{00}$) of the informational and power buses of the functional unit and technical state ($S^{00}$) of it, which cause down state of the output bus, are not represented in this matrix with the purpose of simplifying its form.

The Cartesian product of states of appropriate channels is formed for the state matrix referred to the unit equipped with a number of information, power and output buses. Generally, each element $(S_j)$ of the set $(S)$ of technical states of the unit includes several states, as follows:

$$S_j = (S_{j1}, S_{j2}, ..., S_{ju}),$$

where $u$ is the number of possible technical states.

Probability of the fact that the functional unit control bus is in the j state $(W_j^1)$ is determined, as follows:

$$P(W_j^1) = P(Y_h)P(Z_g)P(S_b), \quad (4)$$

where indices h, g, b comply with the mapping $[Y_h \times Z_g] \times S_b \xrightarrow{F} W_j^1$;

and $P(Y_h)$, $P(Z_g)$, $P(S_b)$ are probabilities of appropriate states.

Probability of up state of the unit output bus is equal to the sum of probabilities (4), and it is determined by the following formula:

$$P(W^1) = \sum_{j=1}^{N_p} P(W_j^1), \quad (5)$$

where $N_p$ is the number of states which result in up state of the unit output bus, (for example, the unit complying with the matrix represented in Table 1 corresponds to the number of states $N_p = 15$).

When a system comprises M units equipped with common information and power buses, the set of up states of output buses is derived from the following expression:

$$W = \bigvee_{m=1}^{M} \{[Y \times Z] \times S_m \xrightarrow{F_m} W_m^1\}. \quad (6)$$

For example, in the case of two two-out-of-three majority elements, probability of up state of an output bus is calculated according to the following formula:

$$P(W) = P(Y^{111})P(W/Y^{111}) + P(Y^{110})P(W/Y^{110}) + P(Y^{101})P(W/Y^{101}) + P(Y^{011})P(W/Y^{011}), \quad (7)$$

where $P(W/Y^{111})$, $P(W/Y^{110})$, $P(W/Y^{101})$, $P(W/Y^{011})$ - are conventional probabilities, and they are represented as follows:

$$P(W/Y^{111}) = P(Z^{111})\prod_{i=1}^{2} P(S_{i,\Sigma}) + P(Z^{110})\prod_{i=1}^{2} P(S_{i,\Sigma}^{110}) + P(Z^{101})\prod_{i=1}^{2} P(S_{i,\Sigma}^{101}) + P(Z^{011})\prod_{i=1}^{2} P(S_{i,\Sigma}^{011}),$$

$$P(W/Y^{110}) = [P(Z^{111}) + P(Z^{110})]\prod_{i=1}^{2} P(S_{i,\Sigma}^{110}),$$

$$P(W/Y^{101}) = [P(Z^{111}) + P(Z^{101})]\prod_{i=1}^{2} P(S_{i,\Sigma}^{101}),$$

$$P(W/Y^{011}) = [P(Z^{111}) + P(Z^{011})]\prod_{i=1}^{2} P(S_{i,\Sigma}^{011}),$$

$$P(S_{i,\Sigma}) = P(S_i^{111}) + P(S_i^{110}) + P(S_i^{101}) + P(S_i^{011}), \quad P(S_{i,\Sigma}^{110}) = P(S_i^{111}) + P(S_i^{110}),$$

$$P(S_{i,\Sigma}^{101}) = P(S_i^{111}) + P(S_i^{101}), \quad P(S_{i,\Sigma}^{011}) = P(S_i^{111}) + P(S_i^{011}).$$

4. The hierarchical levels following in consecutive order are formed, and up state probabilities of appropriate output buses of functional units are calculated.

As a result of executing the above procedure, up state probability of output buses of the information control system (ICS), i. e. required measure of failure-free operation, which is probability of failure-free operation (reliability function) of ICS, is determined.

Reliability measures calculation for stationary apparatus of stations and stages of the integrated safety and automated control system for St.-Petersburg Metro train traffic has been made by adopting this method. A fragment of the block-diagram of this bus-structured system is shown in Figure 2. Appropriate conventional signs shown in Figure 2 are given in Table 2.

Table 2. Names and conventional signs of units.

| Unit name | Sign |
|---|---|
| Workstation | WS |
| Arrival/departure unit | ADU |
| Power supply unit | PSU |
| Track circuit PM communication channel apparatus unit | PU |
| Adjacent station PM communication channel apparatus unit | PMU |
| Switch point control unit | SCU |
| Light signal control unit | LSCU |
| Power distribution unit | PDU |
| Output filter unit | OFU |
| Station-based device unit | SDU |
| Arrival/departure unit | ADS |
| Radio modem | RM |
| Station-based digital computing system | SDCS |
| Arrival/departure device | ADD |

Concrete results of performed reliability calculation (including the list of functional units mounted on the boards and racks of this system) are submitted in the monograph of scientists and specialists of the "Research Institute of Fine Mechanics" Joint-stock company [2].

The analytical-tabular calculation method can be used in the process of predicting reliability of bus-structured complex diagnostic and information systems for medicine and safety systems for thermal and nuclear power engineering.

.

REFERENCES

1. E. J. Henley, H. Kumamoto. Reliability engineering and risk assessment. Prentice-Hall, Inc. Englewood Cliffs, N. J. (1981).

2. Y. V. Antonov, V. P. Belov, A. D. Golyakov and etc**.** Reliability and safety of information control systems (estimation and verification methods). "NII TM" JSC. St.-Petersburg (2004) (in Russian).

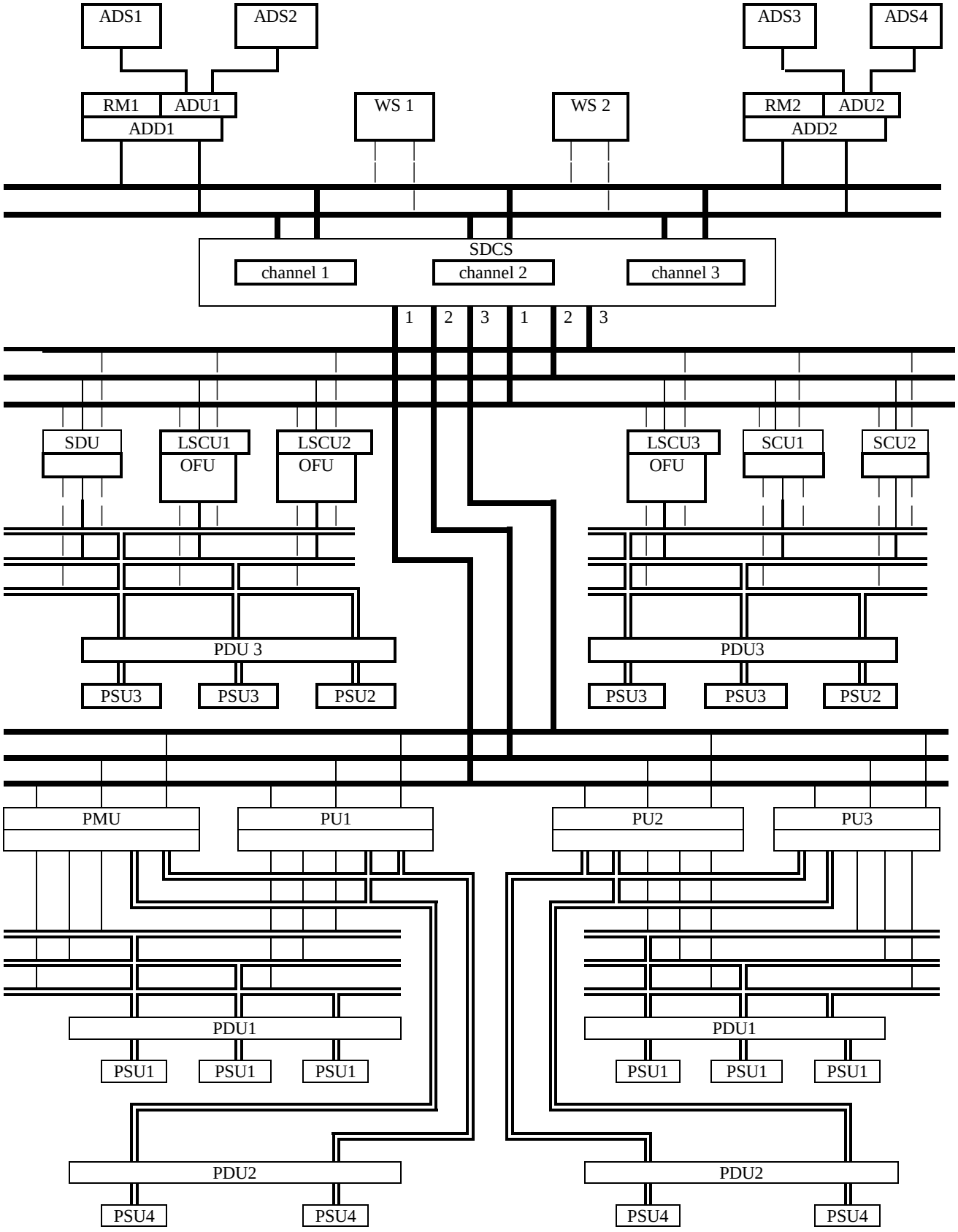


Figure 2. Fragment of block diagram of stationary apparatus of “Dvizheniye” system

Information on authors of report

**“Analytical-Tabular Calculation Method of Reliability Measures and its Application in Process of Estimating Failure-Free Operation of Metro Safety Systems”**

Yuriy V. Antonov
Kandidat of Technics
Chairman of Board of directors of the “Research Institute of Fine Mechanics” Joint-stock company

Viktor P. Belov
Kandidat of Technics, senior lecturer
Director General and Cief Designer of the “Research Institute of Fine Mechanics” Joint-stock company

Aleksey D. Goljakov
Doctor of Technics, professor
Main Expert of the “Research Institute of Fine Mechanics” Joint-stock company

Sergey J. Starkov
Chief of reliability service of the “Research Institute of Fine Mechanics” Joint-stock company

The postal address: 47 Nepokoryonnikh Prospect,
St.-Petersburg, 195256,
Russia
Contact telephones: 535-19-12, 535-17-00
Fax: (812) 535-83-74
E-mail: Golyakov@niitm.spb.ru