Original article
https://doi.org/10.21683/1729-2646-2022-22-1-4-12

Analysing the effect of information redundancy on the dependability indicators of distributed information systems

Vladimir V. Kulba[1], **Sergey K. Somov**[1]*, **Alexey B. Shelkov**[1], *Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russian Federation*
**ssomov2016@ipu.ru*


Vladimir V. Kulba


Sergey K. Somov


Alexey B. Shelkov

Abstract. Aim. *The paper analyses the effect of information redundancy on the functional dependability indicators of distributed automated information systems. Information redundancy in the form of hot standby and HDD archives located in the system nodes is examined.* **Methods.** *The concepts of the probability theory and Markov processes are employed.* **Results.** *Indicators of operational dependability of distributed information systems and the effect of operational and recovery redundancy of data sets on these indicators are analysed. The paper analyses the efficiency of three backup strategies in distributed systems.* **Conclusions.** *Using information redundancy significantly improves the dependability and operational efficiency of distributed systems. At the same time, this type of redundancy requires a certain increase in operating costs.*

Keywords: *distributed information systems, data backup and recovery, failures, faults, dependability indicators of information systems.*

For citation: *Kulba V.V., Somov S.K., Shelkov A.B. Analysing the effect of information redundancy on the dependability indicators of distributed information systems. Dependability 2022;1: 4-12. https://doi.org/10.21683/1729-2646-2022-22-1-4-12*

Received on: *06.10.2021* / **Upon revision:** *07.02.2022* / **For printing:** *18.03.2022.*

Introduction

Today, information technology is a key element of the managerial control infrastructure that allows improving its efficiency, minimizing the cost of various resources, stimulating labour productivity and other management performance indicators.

The operational dependability of any automated information system significantly depends on the integrity of the data it uses. The matter of ensuring a high system dependability and integrity of the data it uses is of particular relevance for large, geographically distributed multi-level systems of various purpose, such as most advanced information systems operated by the Russian Railways, e.g., KASANT, the Automated System for Tracking, Supervision and Elimination of Technical Failures and Dependability Analysis [1].

Connecting hundreds and thousands of computers with communication channels into large-scale computer networks of various scales and topologies allowed creating distributed automated information systems (DAIS) that, compared with local systems, have acquired qualitatively different features and capabilities [2, 3].

Among other things, the integrity of data stored on multiple storage media may be affected by various negative factors [4]. Such factors may include: errors and malfunctions [5] of computer equipment, software errors, operator errors caused by non-observance of guidelines and regulations. Errors in the operation of data storage devices may cause distortion and even loss of data, failure of individual or several network nodes and, in severe cases, of an entire distributed system. In such cases, significant resources and time may be required to restore corrupted data.

The use of information redundancy in distributed information systems is one of the efficient methods for ensuring high data integrity and dependability of such systems. Currently, information redundancy is widely used in the form of two types of data redundancy [3, 6]:

- online redundancy that consists in creating online backup (OB) data from a certain set of copies and/or historical data arrays that are used to improve the reliability of processing of incoming inquiries by the distributed system in the event of data errors or their partial loss during inquiry processing;

- recovery redundancy that consists in creating special recovery backup (RB) data that are used only for restoring real-time data if they are affected by corruption or errors.

Second, since the examined information systems have a distributed geospatial topology, two primary methods of storing the two types of backups can be used, i.e., centralized and decentralized. In case of centralized storage, the backup is located in a single, central node of the system. In case of decentralized storage, the data backup is located in several system nodes selected in accordance with a certain backup localization algorithm [6].

Third, if the number of system nodes is high, there are many options for backup allocation, which complicates the choice of the best configuration. That causes the requirement to define and solve the problem of selecting the best backup allocation.

Fourth, when looking for the best allocation of distributed backup across network nodes, various parameters of the network itself need to be take into consideration. Those include the bandwidth of communication channels, traffic and average message latency, cost of using computers and network channels, etc.

Strategies for online backup and redundancy

Today, three online redundancy strategies are used to ensure the integrity of data that take into account the specifics of their use in information systems [3]:

Strategy I. According to this strategy, a backup is created and then used that consists of a certain number of copies of the permanent (rarely modified) data array. Processing of each inquiry to the array's data starts with the main array. If the array is corrupted, the inquiry is processed using the data from the first copy, and so on.

Strategy II. This strategy uses a backup that includes a certain number of historical versions of an array with frequently modified data. Array history AP_i is its exact copy created at time t_i $\left(i = \overline{1, N}\right)$ and the change log of the array's data that occurred within the time interval $(t_i+\Delta t)$. In case the main array is corrupted, it is restored using history AP_N. If the history is corrupted in the course of restoration, it is restored using history $AP_{(N-1)}$.

Strategy III. This strategy is mixed and restores the corrupted main array first by using copies of the array (according to strategy I), and, if all copies are corrupted, by using the backup from the history (according to strategy II).

The use of OB significantly increases the dependability of the distributed system when processing inquiries, but does not completely eliminate the possibility of the OB itself becoming corrupted. The recovery backup data (RB) is used for restoring a corrupted OB. There are two main options for using the RB [6]:

1) The first option is used in case of decentralized allocation of OB in several system nodes. If an OB is corrupted in a certain node of the system, it is restored using another uncorrupted instance of the OB located in the nearest node. In this case, this OB is used as an RB.

2) The second option involves using a special RB, the magnetic media archive (MMA). The MMA is used only for processing inquiries to restore a corrupted OB. The MMA may be hosted in a single network node or multiple instances of it can be hosted in multiple nodes.

The paper examines two strategies for restoring a corrupted OB, i.e., B-1 and B-2 that help significantly improve data integrity in distributed systems [7]. According to strategy B-1, all copies of data arrays that are required for

OB restoration are created sequentially based on RB data. The second strategy, B-2, differs from the first one in that, when obtaining the next copy, data is used not only from RB, but also all previously obtained copies of the data array to be restored.

Operational dependability indicators of a DAIS that uses online backup for restoring corrupted data

Let us consider the primary indicators of operational dependability of a DAIS that, for the purpose of improving such dependability, uses only online backup with no MMA.

In terms of dependability, the operation of a DAIS, in whose nodes an online data backup is hosted, can be represented as a process of such system's transition within the space of possible states. System transitions from one state into another occur as a result of failures of system nodes that process incoming data inquiries and/or after the restoration of previously failed nodes. Thus, the state of a DAIS at any given time can be characterized by the number of failed and that of operable nodes.

When a certain system node processes a data inquiry, the OB of such node may become corrupted. As the result, the node becomes inoperable and no longer able to process incoming inquiries. The node's transition into such state will be considered a failure of the node. Since the system under consideration does not use recovery redundancy, the failed node will remain in this state. Let us assume that after a node fails, all incoming inquiries will be evenly distributed for processing among all still operable system nodes with an OB. In case all redundant nodes fail, the system will become unable to process incoming inquiries. Such state of a DAIS we will also interpret as system failure.

Let us denote by M the number of DAIS nodes hosting online backup, and by H the set of all DAIS states. Set H consists of the following elements: H_0, all system nodes are operable, H_m, m-th node failure, H_{mn}, failure of nodes m and n, $H_{1,2,...,M}$, all M system nodes with an OB failed, system is inoperable.

Then, set H of all system states and its power $|H|$ will be equal to:

$$H=\left\{H_0,H_1,\ldots,H_M,H_{1,2},\ldots,H_{1,2,\ldots,M}\right\},\ |H|=\sum_{i=0}^{M}C_M^i=2^M.$$

At any moment in time t, the system may be only in one state $\xi(t)=H(t)\in H$. Let us assume that the DAIS may remain in the initial state or transition into another state at regular time intervals. At the end of each such period of time, with a certain probability, the system either transitions into another state (one or more nodes failed simultaneously) or remains in the same state (none of the nodes failed). Such transitions between possible system states are called steps of a random process. We denote by $\xi(t)$, $t\geq 0$ the random value that describes the process of a system transitioning from one state into another.

Let us assume that at the moment of time t the system is in state $\xi(t)$. Let us assume that, within a single time interval, node j processes $\lambda_j(t)$ inquiries, provided that the system is in state $\xi(t)$.

Let us also assume that at the initial moment of time t_0 the system is fully operable and has no failed nodes. Let us denote by $\xi(t_0)=H(t_0)$ the initial operable system state at the moment of time t_0, and by $\lambda_j^0=\lambda_j(t_0)$ the number of inquiries that node j is processing at the moment of time t_0.

After a certain period of system operation time operable, node j, at the moment of time t, will be processing $\lambda_j(t)$inquiries:

$$\lambda_j(t)=\lambda_j^0+M_P^{-1}(t)\sum_{i\in I_O(t)}\lambda_i^0. \quad (1)$$

In formula (1), $I_o(t)$ is the set of numbers of the system nodes that failed by time t, while $M_P(t)=M-\left|I_O(t)\right|$ is the number of system nodes hosting a backup that are operable at time t.

When processing a single inquiry in node j, a failure may occur with probability Q_j. Then, for a single time interval $(t, t+1)$, probability $\tau_j(t)$ of node j failing and probability $\beta_j(t)$ of no failure will be, respectively, equal to:

$$\tau_{j(t)}=1-P_j^{\lambda_j(t)};\ \beta_j(t)=1-\tau_{j(t)}=P_j^{\lambda_j(t)};\ P_j=1-Q_j. \quad (2)$$

By sequentially numbering all the elements of set H we obtain set S of system states that consists of the same number of elements:

$$H=S=\left\{S_0,S_1,\ldots,S_M,S_{M+1},\ldots,S_N\right\},\ N=2^M.$$

The above system transition from one state into another is a homogeneous process, as the future state of the system does not depend on its previous transitions, but only on its current state [8, 9]. Then we can state that conditional probability $P\left\{\xi(t)=S_j/\xi(u)=S_i\right\}$that the system, at moment t, is in state S_j, provided that the system, at moment u, was in state S_i, will be equal to:

$$P\left\{\xi(t)=S_j/\xi(t_1)=S_{i_1},\ldots,\xi(t_n)=S_{i_n},\xi(t_u)=S_i\right\}=$$
$$=\left\{\xi(t)=S_j/\xi(t_u)=S_i\right\}=p_{ij}(t-u).$$

At the same time:

$u>t_n>\ldots>t_1;\ t>u;\ i,j\in\left\{0,1,\ldots,N\right\}$.

That means that conditional probability $P\left\{\xi(t)=S_j/\xi(u)=S_i\right\}$ does not depend on moments of time t and u, but depends on distance $(t–u)$ between such moments. Therefore, such conditional probability depends on the time interval from moment u to moment t.

Let us suppose that $p_{ij}(t–u)$ is the conditional probability of an event that corresponds to the transition of the system from state S_i into state S_j within a time interval equal to $(t–u)$. Let us assume that the system's transitions from one state into another occur within a single time unit. Then, the difference between the moments of time t and u will be equal to 1 $(t–u=1)$, while the conditional probability $p_{ij}(t-u)=p_{ij}(1)=p_{ij}$ is the transition probability of the system for states S_i and S_j.

The values p_{ij} of transition probabilities of the examined process will be calculated using the formula:

$$p_{ij} = \begin{cases} 0, \text{ if } (i < j) \text{ or when } \xi(t) = S_j \neq S_i = \xi(t-1) \\ \text{and } |I_0(t)| = |I_0(t-1)|; \\ \prod_{n \in R} \tau_n(S_i) \left[\prod_{n \in R} \beta_n(S_i) \right]^{-1} \prod_{n \in I_p(S_i)} \beta_n S_i, \text{ if other wise.} \end{cases} \quad (3)$$

Formula (3) uses the following notations:

$I_0(t)$, set of numbers of system nodes that failed by time t.

$I_p(S_i)$, set of numbers of operable nodes of a system that is in state S_i;

$\tau_n(S_i)$, probability of failure of node n per unit of time when the system is in state S_i;

$R=[I_0(S_i) - I_0(S_j)]$, set of numbers of the nodes that failed during the transition of the system between two states;

$I_p(S_i)$, set of numbers of the nodes that are operable in system state S_i.

$$\beta_n(S_i) = \tau_n(S_i).$$

In the examined process, the system transitions between various states can be formally represented as an oriented graph. The system states in the graph are represented by its vertices, while oriented arcs correspond to the system's transitions between states (vertices of the graph).

Fig. 1 shows an example of an oriented graph of a random system transition process. The system consists of M = 2 nodes with multiple states: $S_0=H_0$; $S_1=H_1$; $S_2=H_2$; $S_3=H_{1,2}$; $\xi(t_0)=S_0$.

Since the failed nodes are not restored in this case, the system can be considered a non-restorable item that has a finite set of operable states and one state of complete failure [8, 9]. The process of system transition between the different states is an absorbing discrete-time Markov chain [9, 10].

Let us examine the following important indicators of system dependability: T_1, mean time to failure; $Q(t_0)$ and $Q(t,t+t_0)$, probability of system failure within time intervals $[0,t_0]$ and $[t,t+t_0]$; $P(t_0)$ and $P(t,t+t_0)$, probability of no failure within time intervals $[0,t_0]$ and $[t,t+t_0]$;

Let us deduce and analyse the above dependability indicators for the case of a system that operates based on a homogeneous directly connected network (for the situation of a heterogeneous network, the indicators are deduced and analysed similarly using formulas (1)–(3)).

Let us denote by $S=\{S_0, S_1, \ldots, S_N\}$ the set of all states of a system, whose set of nodes with online backup is equal to N. Let us denote by S_j such system state, in which j nodes with online backup have failed. Let the initial rate of inquiries processed by each node of the system in state S_0 be equal to λ_0. The the rate of inquiries processed by network nodes that are operable in system state S_j will be denoted as λ_j. Then, in accordance with formula (1), we obtain the following formula for calculating λ_j:

$$\lambda_j = \lambda_0 + \lambda_j (N-j)^{-1} = \lambda_0 N (N-j)^{-1}. \quad (4)$$

The probability τ_j that, within a single time interval, one of the nodes of the network in state S_j fails – taking into account formula (2) – will be calculated as follows:

$$\tau_j = 1 - p^{\lambda}. \quad (5)$$

The transition probabilities for the examined network, taking into account (3), will be calculated using the following formula:

$$p_{ij} = \begin{cases} 0, \text{ if } i < j; \\ C_{N-j}^{j-i} \tau_i^{j-i} \beta_i^{N-j}, \text{ if } 0 \le i \le j \le N. \end{cases} \quad (6)$$

Since the system does not use recovery redundancy, the failed node is not restored, and the system will eventually enter state S_N, in which all system nodes will be inoperable. Moreover, p_{NN}=1, since S_N is an absorbing state.

Thus, as a result, we have the matrix $P=p_{ij}$ of probability of system transition between states, initial state of the system S_0 is known, the system has one absorbing state S_N and a set $\{S_0, S_1..., S_{N-1}\}$ of operable states. Then, it can be affirmed that there is an absorbing discrete-time Markov chain. The set $S^1=\{S_0, S_1..., S_{N-1}\}$ of non-recurrent states is defined for it. I.e., the set of operable system states, in which not all nodes have failed. As well as a single-element set of absorbing states $S^2=\{S_N\}$ (when all system nodes are inoperable).

Since a Markov chain has a single absorbing state, it will eventually transition from the initial state into such absorbing state. Let us identify the mean number n_{ij} of steps, after which the chain will be in one of the non-recurrent states $S_j \in S^1$ before absorption, provided that state S_i was its initial state. Each step from state to state takes the system a unit time interval. Hence, value n_{ij} can be considered the mean time the system spends in state S_j before absorption, provided that S_i was the initial state of the system. The initial state S_i itself brings to value n_{ij} a contribution equal to 1 if $i=j$ and 0 if otherwise, i.e.:

$$\delta_{ij} = \begin{cases} 1, \text{ if } i = j; \\ 0, \text{ if } i \neq j. \end{cases}$$

The chain enters state S_m in one step from state S_i with probability p_{im}. If we assume that $S_m \in S^2$, then the chain will never transition into state S_j. If $S_m \in S^1$, then, in the course of n_{mj} steps, the chain will be in state S_j. Hence, we can write:

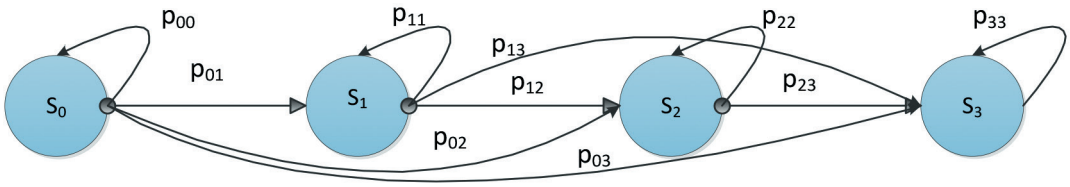

Fig. 1. Graph of the random transition process for a system of 2 nodes

$$n_{ij} = \delta_{ij} + \sum_{S_m \in S^1} p_{im} n_{mi}.$$

This equality in matrix form looks as follows:

$$\tilde{N} = I + \bar{Q}\tilde{N} \text{ or } \left(I - \bar{Q}\right)\tilde{N} = I.$$

In this formula, $I=\delta_{ij}$ is the identity matrix corresponding to the Kronecker delta of dimension $(N\times N)$; $\bar{Q}$ is a trix of dimension $(N\times N)$ that describes the chain's behaviour in the set of non-recurrent states S^1. It is derived from matrix $P=p_{ij}$ by removing the last column and the last row.

We will derive the fundamental matrix $\tilde{N}$ for the absorbing Markov chain by premultiplying by $\left(I - \bar{Q}\right)^{-1}$ both parts of the above equation [10]:

$$\tilde{N} = \left(I - \bar{Q}\right)^{-1}. \quad (7)$$

Let us identify the mean time t_i of the chain being in the set of states S^1 by using matrix $\tilde{N}$, given that the initial state of the chain is state S_i. Obviously, $t_i=0$ if $S_i \in S^2$. Therefore:

$$t_i = \sum_{S_j \in S^1} n_{ij}; \ \ S_i \in S^1. \quad (8)$$

The validity of formula (8) follows from the fact that it is based on the premise that the time the chain remains in the set of states S^1 is equal to a sum of random variables. Or, in other words, it is equal to the sum of each of the individual times of the chain remaining in each of the non-recurrent states of set S^1. Moreover, the value of the mean sum of random variables is always equal to the sum of the mean values that make such sum [11].

As previously identified, $p_{ij}(n)$ is the probability of the system transitioning from state S_i to state S_j in n steps. Then, taking into account the total probability formula, we will deduce that this probability is calculated using the formula:

$$p_{ij}(n) = \sum_{S_m \in S^1} p_{im} p_{mj}(n-1); \ \ p_{mj}(0) = \delta_{mj}.$$

The resulting formula in matrix form will be as follows: $P(n)=P^n$. In other words, the probability matrix of system transitions in n steps is equal to the n-th power of the system's transition probability matrix.

Within the time interval from 0 to t_0, the system will complete t_0 steps, since, in a unit interval, the system completes one transition step. Then, given that $p_{0N}(n)=0$ if $n<N$, we deduce:

$$P(t_0) = 1 - \sum_{n=N}^{t_0} p_{0N}(n); \ Q(t_0) = \sum_{n=N}^{t_0} p_{0N}(n).$$

According to the conditional probability formula, probability of no failure $P(t,t+t_0)$ within the interval between t and $(t+t_0)$ is defined as $P(t+t_0)=P(t+t_0)/P(t)$. It follows that the probability of system failure $Q(t+t_0)$ within the interval between t and $(t+t_0)$ will be equal to $Q(t+t_0)=1-P(t+t_0)/P(t)$.

Using formula (8), let us identify the value of the system's mean time to failure T_1. Since, in our system, the initial state is S_0, while the absorbing state is S_N, the sought time T_1 is identified using formula:

$$T_1 = t_0 = \sum_{S_j \in S^1} n_{0j} = \sum_{j=0}^{N-1} n_{0j}.$$

If, for the examined Markov chain, matrix $\tilde{N} = n_{ij}$ is calculated using formula (7), we will deduce:

$$n_{ij} = \begin{cases} 0, \text{ if } j < i; \\ \prod_{m=i}^{j-1} p_{m,m+1} \left[\prod_{n=i}^{j} (1 - p_{nn}) \right]^{-1}, \text{ if } i \le j. \end{cases}$$

Since, in this case, $n_{ii}=(1-p_{ii})^{-1}$, we will deduce that the system's mean time to failure T_1 is equal to:

$$T_1 = \prod_{j=0}^{N-1} \prod_{m=0}^{j-1} p_{m,m+1} \left[\prod_{n=i}^{j} (1 - p_m) \right]^{-1}.$$

Let us assume that the system's parameters and the value of the unit time interval are such that the probability of an event consisting in a simultaneous failure of two or more system nodes is close to zero, i.e.:

$$p_{jj} + p_{j,j+1} \gg \sum_{n=2}^{N-j} p_{j,j+n}; \ \left(p_{jj+p_{j,j+1}} = 1\right). \quad (9)$$

Given that assumption, let us consider value T_1 of the system's mean time to failure. Fig. 2 shows the transition graph for the system that corresponds to the examined assumptions.

Having defined matrix $\tilde{N}$ using formula (7), we will deduce: $n_{jj}=1$ if $i>j$ and $n_{jj} = p_{j,j+1}^{-1}$ if $i \le j$. Then, the system's mean time to failure T_1 is equal to:

$$T_1 = \sum_{j=0}^{N-1} p_{j,j+1}^{-1} = \sum_{j=0}^{N-1} \left(1 - p_{jj}\right)^{-1}.$$

Let consider the probabilities $\rho_{jj}^{\gamma} \left(\gamma = I, II, II\right)$ of an event that consists in the fact that the system does not leave state S_j within a single time interval. The system nodes use OB created in accordance with one of the three backup strategies $\left(\gamma = I, II, II\right)$. Let us prove that relation (10) is true for the examined probabilities

$$\rho_{jj}^{I} > \rho_{jj}^{III} > \rho_{jj}^{II}. \quad (10)$$

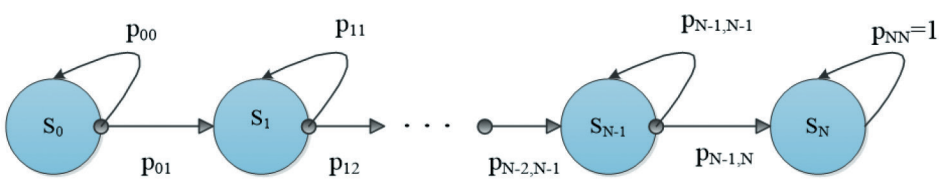

Fig. 2. Graph of a random transition process of a system in a set of states S

Taking into account formulas (4)–(6), we deduce:

$$\rho_{jj} = \beta_j^{(N-j)} = p^{\lambda N};\ j = 0,1,\ldots,(N-1). \qquad (11)$$

In [7], it was proved that, if OB was created using the three online backup strategies $(\gamma = I, II, II)$, for the probabilities P^{γ} of successful processing of inquiries (if the OB of the node, in which the inquiry is processed, is not corrupted), the following formula is true:

$$P^{I} > P^{III} > P^{II}.$$

Then, both formula (10), and the expression T_1^{γ} for the mean time to system failure is true as well:

$$T_1^{I} > T_1^{III} > T_1^{II}.$$

The above findings can be formulated as the following statement.

Statement 1. Using backup strategy I for creating OB in distributed systems that do not use recovery redundancy enables the longest mean time to failure compared to the other online redundancy strategies (strategies II, III).

Value $P(t_0)$ of the systems' probability of no failure within time interval $[0,t_0]$, taking into account formula (9) for the examined configuration of distributed system, i.e., with no recovery redundancy, will be equal to:

$$P(t_0) = 1 - p_{0N}(N)\sum_{n=0}^{t_0-N} B^n;$$

$$\text{где: } p_{0N}(N) = \prod_{i=0}^{N-1} p_{i,i+1} = \left(1 - p^{\lambda N}\right)^N;$$

$$B = \sum_{i=0}^{N-1} p_{ii} = Np^{\lambda N}.$$

Moreover, $P(t_0)=0$ if $t_0<N$.

Indicators of operational dependability of a DAIS that uses magnetic media archives for restoring corrupted data

Let us examine the operational dependability indicators of a DAIS that uses recovery redundancy based on magnetic media archives.

A magnetic media archive is a special set or several sets of a certain number of copies and/or histories of data arrays. MMA is stored in one of the system's nodes (centralized archive) or in several nodes in the case of decentralized storage of several identical copies of magnetic media archives. [12]. MMA is used exclusively for restoring OB that has been corrupted in one or more nodes of a distributed system, thus improving the system's dependability.

Let us assume that, when a node with an MMA processes an inquiry for restoring a corrupted online backup, with certain probability, the node with the MMA itself may fail. Taking into account this possibility, let us analyse the operational dependability indicators of the DAIS that uses recovery redundancy in the form of magnetic media archives that themselves may be in a state of failure.

When processing a data inquiry in a node with an OB, the latter may become corrupted resulting in the failure of such node. The operability of the failed node is restored using one of two restoration strategies: B-1 or B-2 using MMA.

A failure of an entire DAIS system will be understood as such system state, whereas all system nodes with an OB and all MMA have failed.

In the state of failure, a DAIS is unable to process incoming data inquiries or restore the operability of nodes with an OB due to the failure of all MMA.

Let us assume that the following assumptions are true: 1) inquiries arriving to a failed node with an OB are not redirected to operable nodes and are not processed until the node has been restored; 2) should a node with an MMA fail, it is not restored; 3) all inquiries for restoring nodes with corrupted OB arriving to the failed node with an MMA are evenly distributed and redirected to other operable nodes with an MMA; 4) inquiries for restoring failed nodes with an OB are evenly distributed among all operable nodes with an MMA.

To describe the operation of such DAIS, we will use a discrete-time homogeneous absorbing Markov chain. Let us assume that the system parameters are such that the probability of failure of more than one node with an OB or more than one MMA over a unit time interval of system operation is close to zero. Given that assumption, let us define set H of information system states $H = \{H_{m,n}\}$, $m = \overline{0,M}, n = \overline{0,N}$.

State $H_{m,n}$ corresponds to a state of the DAIS, in which m magnetic media archives and n nodes with an OB are in

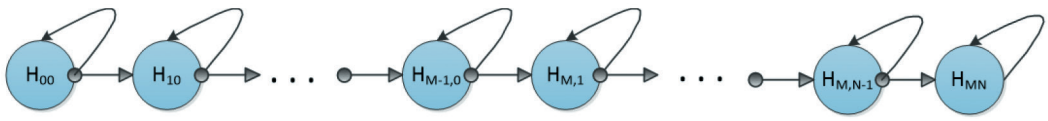

Fig. 3a. Transition graph of a distributed system in a set H of possible states

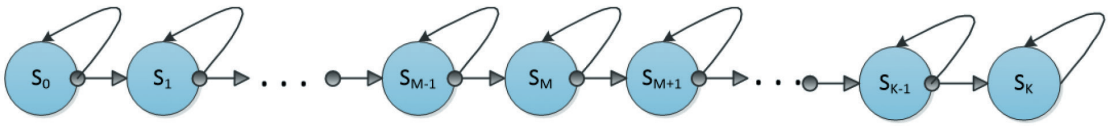

Fig. 3b. Transition graph of a distributed system in a set S of possible states

a state of failure. Let us suppose that, over a unit interval of operation (one-step of the Markov process), the system may transition from state $H_{m,n}$ into state $H_{m+1,0}$ if $n = 0$. While if $m = M$, the system transitions to state $H_{M,n+1}$ or may remain in the initial state. Given the above assumptions, the graph of system transitions will be as shown in Fig. 3a.

Based on set of states H, let us construct set of states $S = \{S_i\}, i = \overline{1,K}$, $K=M+N-1$, where S: $S = \{S_i,\ (i = \overline{1,K}, k = M+N-1)\}$. Element S_i of set S if $0 \le i < M$ is associated with state $H_{i,0}$, while if $i=M$ state $H_{M,1}$ and if $M<i\le K$ state $H_{M,i}$. The constructed set S is associated with the system transition graph shown in Fig. 3b.

Let us assume that, with probability p_{ij}, the system can, in one step, transition from state S_i into state S_j. Given the above assumptions, it can be affirmed that:

$$p_{ij} \neq 0 \text{ if } i = j \text{ or}$$
$$j = i+1,\ p_{kk}=1 \text{ and } p_{ii} + p_{i,i+1} = 1 \text{ if } 0 \le i \le K-1.$$

Let us assume that, within a unit interval, λ data inquiries arrive to each of N system nodes with an online backup. Each node, while a single inquiry is processed, may fail with probability $Q=1-P$ or successfully process it with probability P. Since we have assumed that all inquiries for restoring nodes with an OB are evenly distributed among operable nodes with an MMA, then, if the system is in state S_0, each node with an MMA receives μ_0 restoration inquiries over a unit interval of system operation time:

$$\mu_0 = \lambda Q N M^{-1}.$$

On the other hand, in the course of OB restoration inquiry processing, the MMA itself may become corrupted with probability $Q_A=1-P_A$. Here, P_A is the probability of successful processing in a node with an MMA of an OB restoration inquiry. Should a node an MMA fail, the OB restoration inquiries it received start being evenly distributed among the still operable nodes with an MMA.

Let us suppose that the system is in state $S_i \left(i = \overline{1, M-1}\right)$, then, within a unit interval, each node with an MMA receives μ_i inquiries for restoring corrupted online backups in the network nodes:

$$\mu_i = \mu_0 + i\mu_0 \left(M-i\right)^{-1} = \mu_0 M \left(M-i\right)^{-1}.$$

Then, within a unit interval, an operable MMA in state S_i, may fail with probability φ_i. Probability φ_i is equal to $\varphi_i = 1 - P_A^{\mu_i}$. On the other hand, a node with an MMA can successfully process an inquiry to restore the OB with probability $\Psi_i = 1 - \varphi_i$. The transition of the system in one step from state S_i into state $S_{i+1} \left(i = \overline{1 = M-1}\right)$ occurs with probability $p_{i,i+1}$ that is calculated using the following formula:

$$p_{i,i+1} = 1 - \Psi_i^{M-i} = 1 - P_A^{\mu_0 M} = 1 - P_A^{\lambda Q N};$$
$$p_{ii} = 1 - p_{i,i+1} = P_A^{\mu_0 M}. \qquad (12)$$

Taking into account the findings of the above paragraph, we obtain that the value of probability $p_{i,i+1}$, if $i = M, \left(K-1\right)$, is equal to:

$$p_{i,i+1} = 1 - p^{\lambda N};\ \ p_{ii} = p^{\lambda N}. \qquad (13)$$

Let us assume that, should all nodes with an MMA be corrupted ($i \ge M$), the failed node with an OB is not restored. All data inquiries received by such node are evenly distributed among the still operable nodes with an online backup.

For the examined distributed system configuration, in accordance with formula (7) and taking into account formulas (12) and (13), we obtain the fundamental matrix $\tilde{N} = n_{ij}$ of a Markov chain, in which its element is equal to:

$$n_{ij} = \begin{cases} 0, \text{ if } i > j; \\ p_{j,j+1}^{-1}, \text{ if } i \le j. \end{cases}$$

Next, let us identify the operational dependability indicators of the examined system that uses recovery redundancy in the form of undependable MMA. Nodes with MMA may fail when processing inquiries for restoring a corrupted OB in system nodes. Such distributed system may be considered as a non-restorable item.

Let us assume that the system is in initial state S_0. Then, it can be asserted that the distributed system's mean time to failure T_1 is equal to the mean time T_1 the system will spend in the set of non-recurrent states. The formula for calculating time T_1 is set forth below:

$$T_1 = \sum_{j=0}^{K-1} n_{0j} = \sum_{j=0}^{K-1} p_{j,j+1}^{(K-1)}$$

Taking into account formulas (12) and (13), the formula for calculating T_1 is transformed as follows:

$$T_1 = \sum_{j=0}^{M-1} \left[1 - P_A^{\lambda Q N}\right]^{-1} + \sum_{j=0}^{K-1} \left(1 - P^{\lambda N}\right)^{-1}$$

In [7], for the two restoration strategies B-1 and B-2, inequality $P_A^{B-1} < P_A^{B-2}$ was proved, out of which follows that the following similar inequality for the mean time to failure is true:

$$T_1^{B-1} < T_1^{B-2}.$$

Out of that inequality follows that the following statement is true.

Statement 2. Recovery strategy B-2 in distributed systems that use MMA ensures a mean time to failure greater than recovery strategy B-1.

In [7], it was proved that if OB is created using three backup strategies $\left(\gamma = I, II, II\right)$, for probabilities P^{γ} of successful inquiry processing (if the OB of the node, in which the inquiry is processed, is not corrupted) the below formula is true.

$$P^{I} > P^{III} > P^{II}.$$

If OB in the nodes of a distributed system is created using one of the three backup strategies with redundancy parameters $(x_i > 1, 0 < q_i < 1/2)$, then, in accordance with the findings of [7], for probability (P=1–Q) of successful processing of data inquiry in node i, the following formula is true:

$$P_i^I(x_i) > P_i^{III}(x_i) > P_i^{II}(x_i).$$

Taking this formula into account, the validity of the following inequality is proven:

$$T_1^I > T_1^{III} > T_1^{II}.$$

Let us formulate the findings in the form of the following statement.

Statement 3. Applying strategy I of online backup in distributed information systems enables a mean time to failure greater than that ensured by strategies II and III of online backup.

Let us consider the probability $P(t_0)$ of no failure and the probability $Q(t_0)$ of failure of a distributed system within the time interval $[0,t_0]$.

Based on the earlier findings, we deduce:

$$P(t_0) = 1 - \sum_{n=K}^{t_0} p_{0,K}(n) = 1 - p_{0,K}(K) \sum_{m=0}^{t_0-K} B^m,$$

where:

$$p_{0,K}(K) = \prod_{i=0}^{K-1} p_{i,i+1} = \left[1 - P_A^{\mu_0 M}\right]^M \left[1 - P^{\lambda N}\right]^{(N-1)};$$

$$B = \sum_{i=0}^{K-1} p_{ii} = MP_A^{\mu_0 M} + (N-1)P^{\lambda N}.$$

Within the time interval $[0,t_0]$, the system will fail with probability $Q(t_0)$=1–$P(t_0)$. For time interval $[t,t+t_0]$, the values of probability P of no failure and probability Q of system failure will be calculated using the following formulas:

$$P(t, t+t_0) = P(t+t_0)/P(t);$$

$$Q(t, t+t_0) = 1 - P(t, t+t_0).$$

Conclusion

The paper examines methods for improving the operational dependability of distributed automated information systems by means of information redundancy. An analysis is made of the efficiency of the online backup strategies in nodes of a distributed system and strategies of restoring a corrupted OB. The paper analyses the effect of online and recovery redundancy strategies on such indicators of DAIS operational dependability as the mean time to failure, probability of system failure and probability of no failure within a given time interval. A number of statements regarding the efficiency of the examined strategies in terms of the time of DAIS time to failure were substantiated.

The findings referred to in this paper can be used at the stages of design, development and operation of DAIS of various classes and purposes. These findings may be of particular relevance for such large-scale geographically distributed multi-level automated systems as railway ACS-class systems. For such systems, the problems of ensuring the operational dependability and data integrity become of particular importance and relevance.

References

1. Shestiukov O.S. [Automated system for tracking, elimination supervision of technical failures, dependability analysis]. [Global Trends in Science, Education, Technology: Proceedings of the International Research and Practice Conference]. Belgorod (Russia): Agetstvo perspektivnykh nauchnykh issledovaniy; 2021. P. 42-46. [accessed: 05.02.2022]. Available at: https://apni.ru/article/2543-avtomatizirovannaya-sistema-uchyota-kontrolya. (in Russ.)

2. Shubinsky I.B. [Dependable failsafe information systems. Synthesis methods]. Moscow: Dependability Journal; 2016. (in Russ.)

3. Mikrin E.A., Kulba V.V., editors. [Information support of managerial control systems (theoretical foundations). In 3 parts]. Moscow: Izdatelstvo fiziko-matematicheskoy literatury; 2012. (in Russ.)

4. [Data recovery]. [accessed: 10.09.2021]. Available at: http://www.datarecovery.ru/datarecovery.htm. (in Russ.).

5. Shubinsky I.B, Schäbe H. Errors, faults and failures. *Dependability* 2021;2:24-27.

6. Somov S.K. [Information integrity in distributed data processing systems]. Moscow: ICS RAS; 2009. (in Russ.)

7. Kulba V.V., Somov S.K., Shelkov A.B. [Data redundancy in computer networks]. Kazan: Kazan University Publishing; 1987. (in Russ.)

8. Tikhonov V.I., Shakhtarin B.I., Sizykh V.V. [Random processes. Examples and problems. Volume 1, Random values and processes. Study guide for higher education]. Moscow: Goriachaya liniya – Telekom; 2014. (in Russ.)

9. Rozanov Yu.A. [Random processes]. Moscow: Nauka; 1979. (in Russ.)

10. Kemeny J., Snell J. Finite Markov chains. Moscow: Mir; 1970.

11. Kovalenko I.N., Filippova A.A. [Probability theory and mathematical statistics]. Moscow: Vysshaya shkola; 1978. (in Russ.)

12. Mikrin E.A., Somov S.K. [Analysis of the efficiency of strategies of information recovery in distributed data processing systems]. *Informatsionnye tekhnologii i vychislitelnye sistemy* 2016;3:5-19. (in Russ.)

About the authors

Vladimir V. Kulba, Honoured Science Worker of the Russian Federation, Doctor of Engineering, Professor, Head Researcher, V.A. Trapeznikov Institute of Control Sciences, Russian Academy of Sciences. Address: 65 Profsoyuznaya St., Moscow, 117997, Russian Federation, e-mail: kulba@ipu.ru.

Sergey K. Somov, Candidate of Engineering, Senior Researcher, V.A. Trapeznikov Institute of Control Sciences, Russian Academy of Sciences. Address: 65 Profsoyuznaya St., Moscow, 117997, Russian Federation, e-mail: ssomov2016@ipu.ru.

Alexey B. Shelkov, Candidate of Engineering, Lead Researcher, V.A. Trapeznikov Institute of Control Sciences, Russian Academy of Sciences. Address: 65 Profsoyuznaya St., Moscow, 117997, Russian Federation, e-mail: shelkov@ipu.ru.

The authors' contribution

Kulba V.V. Authored the idea of using information redundancy for ensuring data integrity and operational dependability of information systems. Overall leadership and participation in the preparation of the paper.

Somov S.K. Problem definition. Developed the formal model of an information system that uses online redundancy and magnetic media archives. Analysed the model, proved the assertions set forth in the paper.

Shelkov A.B. Participated in the preparation of the Introduction and the formal system model. Advisory on the specifics of the information systems employed by JSC RZD.

Conflict of interests

The authors declare the absence of a conflict of interests.