Chapter 10

Periodic Monitoring and Recovery of Resources in Information Systems

Alexey Markov, Alexander Barabanov and Valentin Tsirlov

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75232

Abstract

This section deals with the issues of business continuity and recovery after disasters. The authors analyzed standards, laws, and regulations pertaining to the parameters of periodic monitoring and recovery in information systems. This section includes mathematical models of resources and environment periodic monitoring as well as periodic backup and recovery after interruptions or disasters. The work demonstrates that the well-known deterministic periodic monitoring and backup models do not take into account stochastic peculiarities of ergatic systems to the full extent. The authors developed new stochastic models of restricted monitoring and backup that allow taking into consideration resources constrains and random factors of information systems operation. The notion of Bernoulli stream has been introduced. This section suggests the criteria for selecting deterministic or stochastic monitoring and backup models and their combinations. A solution of direct and reverse task of the calculation of control and monitoring procedures frequency is offered. This section also provides a methodology for information system stability management, considering periodic monitoring, rollback, and recovery in case of interruption.

Keywords: business continuity, backup, rollback, recovery, regular procedures, limited stochastic control, Bernoulli flow, stochastic models, deterministic models, periodic inspection, stochastic redundancy

1. Introduction

Basic business continuity planning and disaster recovery procedures include periodic monitoring (control) of resource integrity and periodic backup [1–4].

Requirements for periodic monitoring and backup established by current regulatory documents are briefly described subsequently.

2. Parameters of periodic monitoring and recovery in information systems

2.1. Periodic monitoring parameters

The main parameters of periodic monitoring and recovery in protected information systems (ISs) are provided as follows:

- frequency of monitoring (internal monitoring) of security functions operability of information security controls used in the information systems;
- frequency of external (external audit) of security functions operability of information security controls applied in the information systems; and
- update frequency of the information system parameters and characteristics relating to the information security (change of passwords, update of the information security controls decision rules or signatures).

The results of completed analysis are shown in **Table 1**.

Name of document	Frequency of internal monitoring	Frequency of external monitoring	Frequency of parameters update
ISA 62443–3-3:2013	+	+	+
ISO/IEC 27001:2013/ISO/IEC 27002:2013	+	+	+
PCI DSS	+ (6 months)	+ (6 months)	+ (90 days)
Australian Government Information Security Manual. Controls[1] (Australia)	+	+	+ (90 days)
The IT-Grundschutz Catalogs[2] (Germany)	+	+	+
Cyber Essentials Scheme Requirements for basic technical protection from cyber attacks[3] (Great Britain)	—	—	+
Information Security Provisions in Federal Information Systems[4] (Russia)	+	+	+ (180, 120, 90, and 60 days)
Requirements for Information Security in Process Control Systems (Russia)	+	+	+ (180, 120, 90, and 60 days)
NIST SP 800–53[5]/NIST SP 800-63B[6] (USA)	+	+	+

[1] https://www.asd.gov.au/publications/Information_Security_Manual_2017_Controls.pdf
[2] https://download.gsb.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf
[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/647,619/requirements_archived.pdf
[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
[5] https://nvd.nist.gov/800-53/Rev4
[6] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Table 1. Requirements for the periodicity of control.

2.2. Periodic backup parameters

In practice [1, 2, 4, 5], the main parameter defining the frequency of periodic information backup is the recovery point objective (RPO)—the maximum period of data loss occurring due to an information security incident. The value recovery time objective (RTO) is the period of the information system unavailability in case of the information security incident. The value of RPO defines the backup frequency (**Figure 1**).

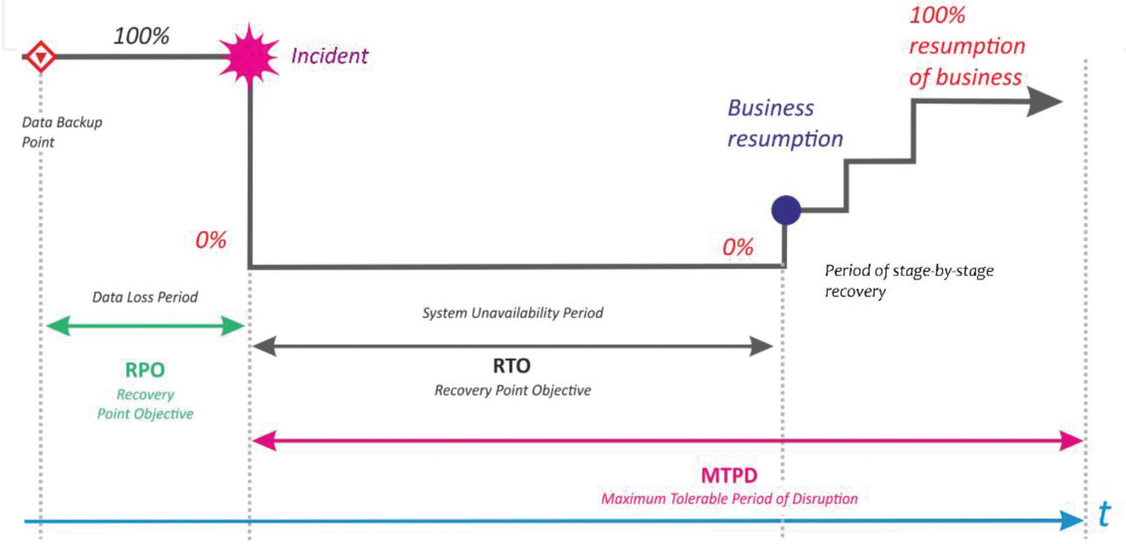

Figure 1. Diagram of the system operation and incident recovery.

Document name	Requirements for periodic backup	Quantitative values or calculation formulae
ISA 62443–3-3:2013	+	—
ISO/IEC 15408	+	—
ISO/IEC 27001:2013/ ISO/IEC 27002:2013	+	—
Australian Government Information Security Manual Controls	+	+
The IT-Grundschutz Catalogs	+	—
Cyber Essentials Scheme Requirements for basic technical protection from cyber attacks	—	—
GOST R 56939	+	—
Information Security Provisions in Federal Information Systems	+	—
Requirements for Information Security in Process Control Systems	+	—
NIST SP 800–53/NIST SP 800–34	+	—
Framework for Improving Critical Infrastructure Cybersecurity[1]	+	—

[1] www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Table 2. Requirements for backup frequency.

The analytical review of regulatory documents and methodologies defining the requirements for information security relating to periodic backup and recovery is shown in **Table 2**.

As the completed review shows (**Tables 1** and **2**), there are clear requirements for periodic monitoring and backup though their main parameters are defined either by expert judgments or by management order.

Considering high subjectivity of such decisions, it is reasonable to develop mathematical models for the calculation of periodic monitoring and backup parameters.

3. Mathematical models of periodic monitoring and backup

As noted earlier, the basic mechanism for providing functional stability to information systems (ISs) is systematic monitoring and backup against possible failures. There are two key approaches to arranging monitoring in IS. The first one relates to the occurrence of a certain event of the computation process (message processing, initiating an exchange among processes, system program call, etc.) [6]. This approach's drawbacks are the difficulty in identifying a set of controlled events of the computation process and the potential for unlimited growth of control points. The latter makes the approach hard to apply during IS normal operation, given the specified resource and task-time restrictions.

The second approach involves a periodic check of the system at predetermined intervals [7–10]. This is consistent with time schedules and allows the existing resource restrictions to be taken into consideration, but fails to fully reflect the stochastic nature of the occurrence of various errors and irregularities. Furthermore, a number of subjective factors make it impossible, in the first place, to organize periodic control in ergatic systems at strictly specified intervals. There is another approach, however, that takes into account the stochastic external factors of IS functional stability, given the specified time and economic constraints.

Under ISO/IEC 15408–1:2009,[1] monitoring covers not only SW (assessment object) but also the operational environment. Let us consider stochastic and deterministic models of the earlier procedures.

3.1. Periodic resource monitoring models

Let us conditionally present the IS software (SW) operating process as alternating flows of errors *I(y)*, normal operation recovery *I(z)*, failures *I(Q)*, and SW/environment control (**Figure 2**).

Being mutually alternative, the flows of failures and normal system operation recovery result from the flow of errors and are shifted with respect thereto by the values *Q(t)* and *z(t)*. The maximum of these values determines the manifestation of a respective flow. Assuming the recovery time to be instantaneous, the normal operation recovery flow may be considered part

[1] ISO/IEC 15408–1:2009: IT—security techniques—evaluation criteria for IT security.

of the control flow. In this case, the task of providing SW functional stability comes down to that of optimizing restricted control that meets the condition $z(t) < Q(t)$.

Let us consider the SW life cycle period t, having regard to the conducted inspection control of repeatable accuracy. Because the period t far exceeds the control time, let us assume the latter to be instantaneous. Then, the SW repeatable accuracy is characterized by the probability $P(\hat{z} < Q) = F\hat{z}\ (Q)$ that the irregularity/vulnerability/error detection time $\hat{z}$ within the inter-control interval is not longer than the permissible SW life cycle period Q, where there is an irregularity. A periodic control fragment is shown in **Figure 3**.

Let us consider the flow of irregularities (errors and vulnerabilities) to be the simplest one with the density of interval ŷ distribution among them:

$$g_{\hat{y}} = \lambda e^{-\lambda y} \tag{1}$$

where λ is the intensity of irregularities.

Let us define a stochastic model for the detection of irregularities. In this case, control is undertaken a certain number of times with equal probability and independently of one another. Thus, the limited flow formed by all the control points is **Bernoulli's flow** with the density of interval $\hat{T}$ distribution among the control points [11]:

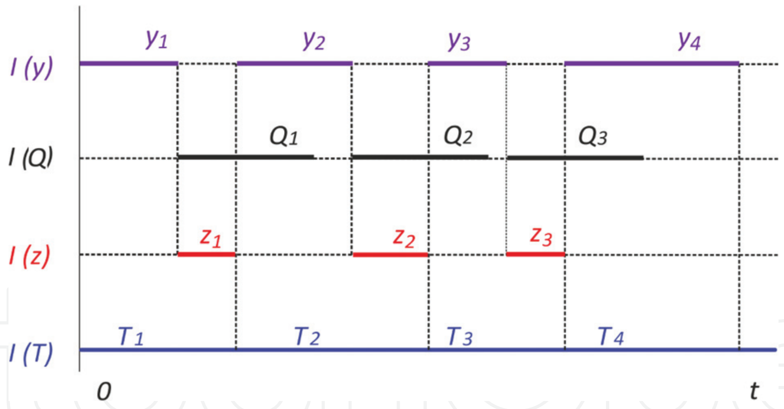

Figure 2. Flows of errors, failures, recovery, and control.

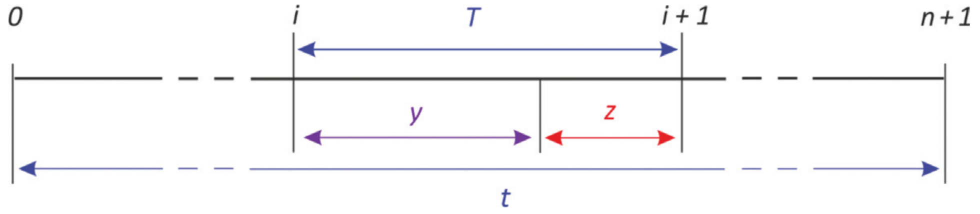

Figure 3. A fragment of the inspection control of an information security tool.

$$f_{\hat{T}} = \mathrm{n/t}(1 - T/t)^{n-1} \tag{2}$$

where n is the number of control points.

The delay time $\hat{z} = \hat{T} - \hat{y}$ is a function of two stochastic variables and has the following distribution function:

$$F^s_{\hat{z}} = \iint_{(S)} \frac{n}{t\left(1 - \frac{T}{t}\right)^{n-1}} \lambda e^{-\lambda y} dTdy; \, (t > 0, n > 0) \tag{3}$$

Having defined the integration limit (**Figure 4**), we obtain the following:

$$\mathrm{F}^{\mathrm{s}}_{\hat{\mathrm{z}}} = \int_0^{\mathrm{t-z}} \left(\int_{\mathrm{y}}^{\mathrm{y+z}} \mathrm{n/t}(1 - \mathrm{T/t})^{\mathrm{n-1}} \, \lambda \mathrm{e}^{-\lambda y} \mathrm{dT} \right) \mathrm{dy} + \int_{t-z}^{t} \left(\int_y^t n/t(1 - T/t)^{n-1} \, \lambda e^{-\lambda y} dT \right) dy \tag{4}$$

After simplifying (Eq. (4)), we have the following formula:

$$F^s_{\hat{z}} = \lambda/t^n \left(\int_0^{t-z} e^{-\lambda y}((t - y)^n - (t - z - y)^n) dy + \int_{t-z}^t e^{-\lambda y}((t - y)^n) dy \right) \tag{5}$$

Having expanded the formula integrands as a power series, we obtain an approximate value of the distribution function that is the basic computational ratio:

$$F^s_{\hat{z}} = \lambda \sum_{i=0}^{n} \sum_{j=0}^{r} \sum_{l=1}^{n+j+1} (-1)^{i+j+l+1} C^i_n C^l_{n+j+1} \frac{\lambda^j t^{j+1-l} z^l}{j!(1 + j + i)} \tag{6}$$

where r is the number of iterations.

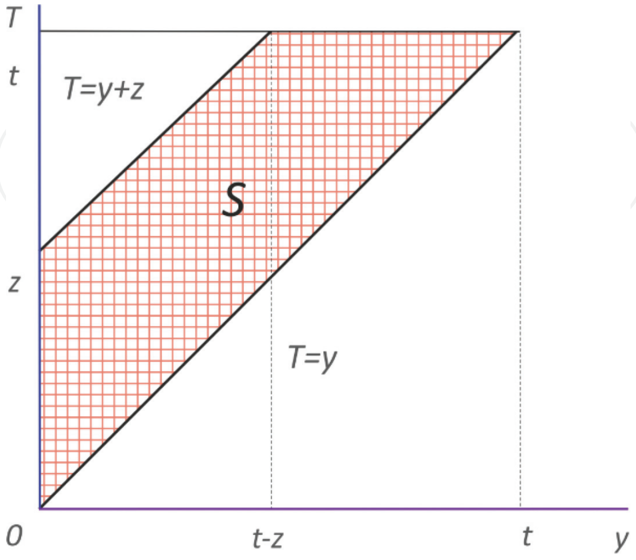

Figure 4. Domain of integrating the irregularity detection time delay interval.

In order to compare stochastic and deterministic models, let us elaborate on the latter. The deterministic model's control points form a regular flow with a constant value of the interval *T = t/(n + 1)* and the irregularity detection time distribution density:

$$g_{\hat{z}} = \lambda e^{-\lambda(T-z)}; \quad (0 < z < T) \tag{7}$$

It can be shown that the expression for the distribution function in the deterministic model is as follows:

$$F_{\hat{z}}^{d} = e^{-\lambda T}\left(e^{\lambda z} - 1\right); \quad (0 < z < T) \tag{8}$$

Comparison of the expressions for the models (Eqs. (4) and (8)) suggests that the models under review conform to the process of detecting SW repeatable accuracy disturbances (at specified values λ, Q, t, and n):

$$F_{\hat{z}}^{s}(z) \lesseqgtr F_{\hat{z}}^{d}(z) \tag{9}$$

The irregularity detection probability P_n for the SW life cycle period t can be presented as follows:

$$P_n = (n+1) \cdot F_{\hat{z}} \tag{10}$$

where n is the number of inspection control points *(n > 0)*, $F_{\hat{z}} = \max\left(F_{\hat{z}}^{s}(z), F_{\hat{z}}^{d}(z)\right)$.

A review of the models discussed earlier showed an advantage of the stochastic model, given a small number of inspection control points. Conceptually, it can be accounted for by the fact that even with a small number of random points of SW characteristics control, there is always a likelihood that an irregularity is detected once it has occurred, whereas in the case of the deterministic model, the inspection period may not be less than the specified value.

3.2. Operational environment periodic control model

The control of restrictions imposed on SW primarily involves inspecting SW environment and operation/production conditions. Such inspections help rule out irregularities (errors, vulnerabilities) concerning the SW front-end interface. In this regard, the procedures for detecting environment irregularities can be interpreted as a mechanism to prevent SW irregularities.

Environment control requirements are specified by ISO 15408 standards.

Let us consider IS operation where an SW error prevention mechanism is available.

When developing environment control models, we will adhere to the approach outlined in the previous section. We will assume SW repeatable accuracy to be characterized by the probability $P(\hat{z} < Q) = F\hat{z}(Q)$ that the preliminary control $\hat{z}$ time between the environment control point and a possible point of occurrence of SW characteristic disturbance does not exceed the permissible time Q. Let us define a stochastic model of environment irregularity control (**Figure 5**).

It can be shown that the preliminary control time is a function of two random values $\hat{z} = \hat{y} - \hat{T}$ and has the following distribution function:

$$F^{s}_{\hat{z}} = \iint_{(S)} \frac{n}{t\left(1 - \frac{T}{t}\right)^{n-1}} \lambda e^{-\lambda y} dT dy; \qquad (t > 0, n > 0) \tag{11}$$

where n is the number of environment control points and λ is the SW characteristic disturbance intensity.

Having defined integration limits (**Figure 6**) and simplified the expression, we obtain the following:

$$F^{s}_{\hat{z}} = \int_{0}^{z} f\hat{T}(T) e^{-\lambda T}\left(1 - e^{-\lambda T}\right) dT + \int_{z}^{t-z} f\hat{T}(T) e^{-\lambda T}\left(1 - e^{-\lambda z}\right) dT + \int_{t-z}^{t} f\hat{T}(T) e^{-\lambda T} dT - e^{-\lambda t}\left(\frac{z}{t}\right)^{n}, \tag{12}$$

Having expanded the formula integrands as a power series, we obtain an approximate value of the distribution function that is the basic computational ratio:

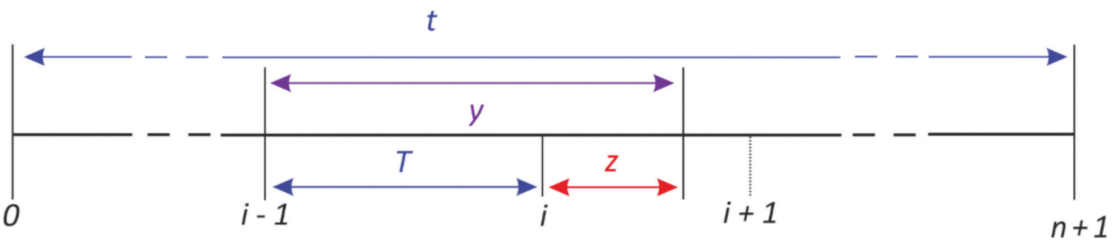

Figure 5. Operation of the system, with an irregularity error prevention mechanism available.

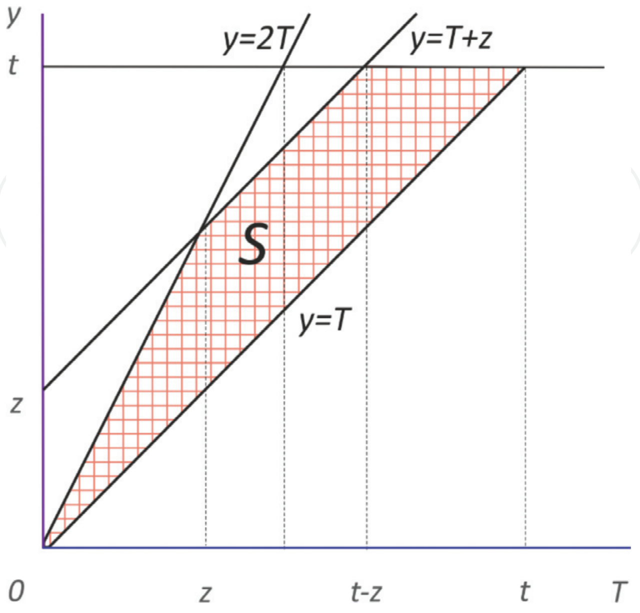

Figure 6. Domain of integrating the irregularity prevention time interval.

$$F_{\hat{z}}^{s} \approx n \sum_{i=0}^{r} \left(\sum_{j=0}^{n-1} b_1 b_2 \right) - e^{-\lambda t} \left(\frac{z}{t} \right)^{n}; \qquad (t > 0, n > 0) \tag{13}$$

where r is the number of iterations; $b_1 = (-1)^{-i+j} C_{n-1}^{i} \frac{\lambda^j}{\left(j! t^{i+1} (i+j+1)\right)}$; $b_2 = t^{i+j+1} - z^{i+j+1}$ $\left(2^j - e^{-\lambda z}\right)(t - z)^{i+j+1}\, e^{-\lambda z}$.

Let us compare the obtained stochastic model and the deterministic one. The deterministic model's control points form a regular flow with a constant value of the interval $T = t/(n + 1)$ and the following preliminary control time distribution density:

$$g_{\hat{z}} = \lambda e^{-\lambda(T+z)}; \qquad (0 < z < T) \tag{14}$$

Hence, the expression for the distribution function in the deterministic model will be as follows:

$$F_{\hat{z}}^{d} = e^{-\lambda T} \left(1 - e^{-\lambda z}\right); \qquad (0 < z < T) \tag{15}$$

By comparing computational model expressions at specified values λ, Q, t, and n, we obtain a criterion to choose a model:

$$F_{\hat{z}}^{s}(z) \lesseqgtr F_{\hat{z}}^{d}(z) \tag{16}$$

The probability P_n of irregularity prevention for SW life cycle period t can be presented as follows:

$$P_n = (n + 1) \cdot F_{\hat{z}} \tag{17}$$

where n is the number of control points $(n > 0)$, $F_{\hat{z}} = \max\left(F_{\hat{z}}^{s}(z), F_{\hat{z}}^{d}(z)\right)$.

Comparative analysis of stochastic and deterministic models showed the former's effectiveness with a small number of control points. Therefore, when managing system information security by numerical methods, it is possible to identify preferred models (stochastic, deterministic, or combined) that bolster confidence in SW. This gives an effect akin to introducing structure redundancy, that is, a special type of redundancy—**stochastic**—the use of which is unlikely to result in higher costs [11].

An example of comparing deterministic and stochastic models is shown in **Figure 7**.

3.3. Periodic backup models

The previous subsections dealt with deterministic and stochastic SW control models. When tackling comprehensive tasks of providing IS operational reliability and security, it is important to ensure information safety in case of incidents. This can be achieved by developing an incident management system.[2]

Apart from control models, this work also investigates backup and recovery models.

The backup mechanism is intended to recover a system's normal operation in case of a failure or an incident, such a recovery starting from the last backup time (**Figure 8**).

The backup mechanism control task boils down to developing a checkpoint (CP) setting model that minimizes the mathematical expectation of the program operation delay time, given the restrictions on the total SW operation time and the number of CP. The issues of minimizing the mathematical expectation of delay time by changing the CP setting frequency and the determined interval among checkpoints are discussed in [9].

Let us consider a situation when an interval is a random value.

If the failure flow of the computation process is regarded as simple, it can be shown that the delay time $\hat{z} = \hat{y} - \hat{T}$ is a function of two random values and has the following mathematical expectation:

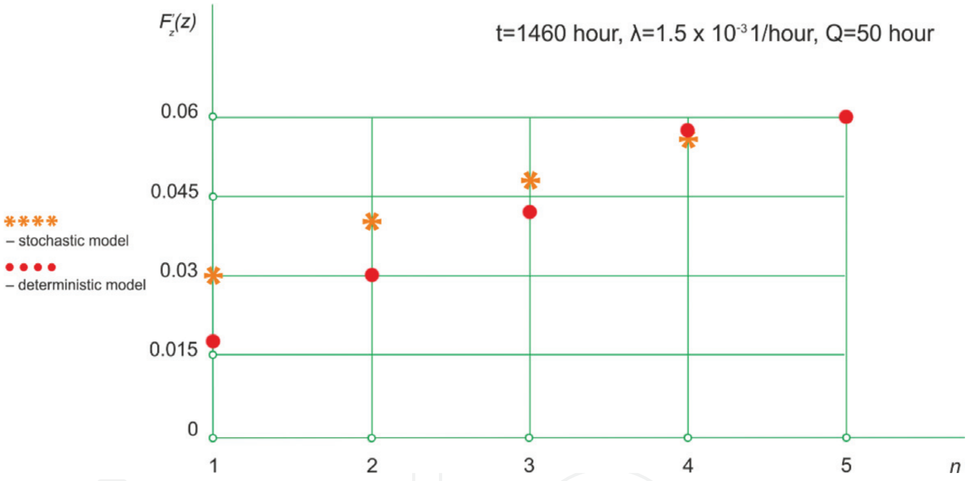

Figure 7. Irregularity prevention probability versus the number of preliminary control points.

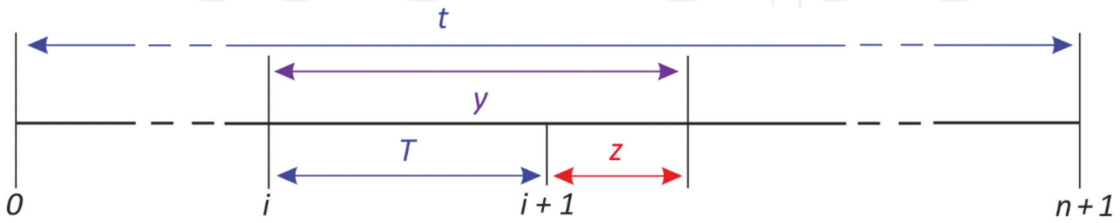

Figure 8. Program operation using a checkpoint mechanism.

[2] ISO/IEC TR 18044:2004 IT—security techniques—information security incident management.

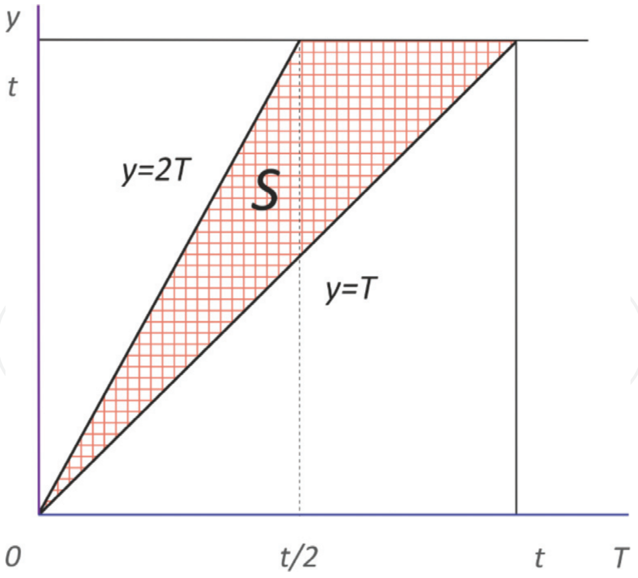

Figure 9. Domain of integrating the program operation delay time interval.

$$M_{\hat{z}}^{s} = \iint_{(S)} (y - T)\frac{n}{t}\left(1 - \frac{T}{t}\right)^{n-1} \lambda e^{-\lambda y} dT dy; \qquad (t > 0, n > 0) \tag{18}$$

where n is the number of environment control points and λ is system's failure intensity.

Having defined integration limits (**Figure 9**) and simplified the expression, we obtain the following:

$$M_{\hat{z}}^{s} = \int_0^t n/t(1 - T/t)^{n-1} \frac{e^{-\lambda T}}{\lambda} dT - \int_0^{t/2} n/t(1 - T/t)^{n-1} e^{-2\lambda T}\left(T + \frac{1}{\lambda}\right) dT - b_1, \tag{19}$$

where $b_1 = \frac{e^{-\lambda t}}{2^n}\left(\frac{1}{\lambda} + nt/(2n + 2)\right)$.

Having expanded the integrands as a power series, we obtain an approximate value of the mathematical expectation of delay time:

$$M_{\hat{z}}^{s} \approx n \sum_{i=0}^{n-1} \sum_{j=0}^{r} (-1)^{j+i} C_{n+1}^{i} \frac{\lambda^j t^j b_2}{j!} - b_1, \tag{20}$$

where $b_2 = \frac{1}{(\lambda(i+j+1))} - \frac{t}{2^{i+2}(i+j+2)} - \frac{1}{2^{i+1}\lambda(i+j+1)}$, r is the number of iterations.

In order to compare the obtained stochastic model (Eq. (20)) and the deterministic one, we consider the latter in more detail. The deterministic model's checkpoints form a regular flow with a constant value of the interval $T = \frac{t}{n+1}$. The delay time distribution density will be as follows:

$$g_{\hat{z}} = \lambda e^{-\lambda(\ T + z)}; \qquad (0 < z < T). \tag{21}$$

It can be shown that the expression for the mathematical expectation of delay time in the deterministic model is as follows:

$$M^d_{\hat{z}} = \frac{e^{-\lambda T}}{\lambda}\left(1 - e^{-\lambda T}(\lambda T + 1)\right); \qquad (0 < z < T) \tag{22}$$

By comparing the expressions (Eqs. (20) and (22)), we obtain a criterion allowing a model to be chosen at specific values λ, t, and n:

$$M^s_{\hat{z}}(z) \lesseqgtr M^d_{\hat{z}}(z) \tag{23}$$

Considering the CP setting time and restart to be instantaneous, we obtain a total SW operation time model, given the availability of the CP mechanism:

$$t'(n) = t + (n+1)M_{\hat{z}} \tag{24}$$

where t is the SW operation time, n is the number of checkpoints, and $M_{\hat{z}} = \max\left(M^s_{\hat{z}}(z), M^d_{\hat{z}}(z)\right)$ is the mathematical expectation of the SW operation delay time in case of failure.

Here is an example using the department archive data for the first half of 2017. The database (DB) was inspected seven times over this period. The inspections revealed 12 errors, all of which were corrected by standard methods, with the relevant entry made in the administrator log. The following error parameters were calculated:

- the average time between errors $M_{\hat{z}}$ = 43.83 h;
- the error intensity λ = 0.022 1/h;
- the average quadratic deviation $\delta_{\hat{z}}$ = 30.04 h; and
- *Cramér-von Mises criterion* (goodness of fit) *k(n)* = 0.55.

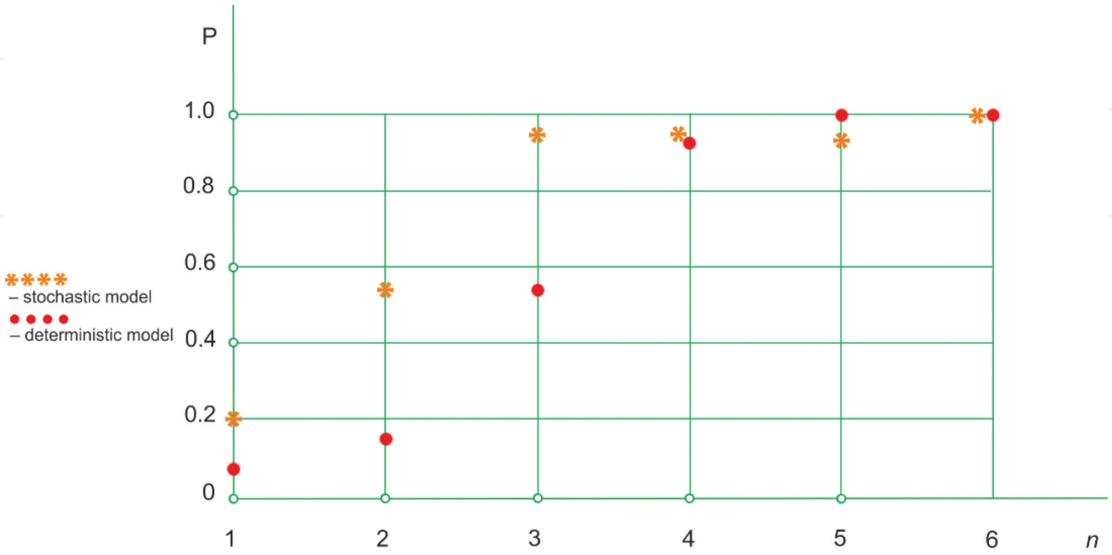

Figure 10. DB error detection probabilities versus the number of control points.

Control type	Number of control points	Man hours	Recovery probability
Conventional	7	42	1.0
Deterministic	4	24	0.99996
Stochastic	3	18	0.99997

Table 3. An example of control parameter calculation results.

This allowed the error flow to be considered a stationary Poissonian flow. A study of the electronic archive DB operation in 2000–2017 showed that the restriction on the correctable error detection time Q was more than 1 month.

The DB recovery probabilities calculated by the formulas (Eqs. (20) and (22)) and their dependence on the number of control points for the first half of 2010 ($t = 1052$ h) are shown in **Figure 10**.

Taking into account the electronic archive availability requirements, it is advisable to use only three control points when applying the stochastic model (**Table 3**).

Thus, the practical solutions offered in this work allow for the stochastic nature of DB errors. This permits the desired error detection model to be chosen at a specified DB and electronic archive parameters.

4. System functional stability management

In general, IS periodic control involves performing a number of standard procedures:

- software error control;
- operational environment error control; and
- backup in case of failure.

Choosing a strategy and the number of control/backup points helps manage the system's stability, integrity, and accessibility levels [12]. For example, considering the earlier procedures, one can define the system availability ratio (operational availability factor [13]):

$$R = \left(\frac{t}{\left(t + M_{n_r}^r\right)}\right)\left(p + (1-p)\,\left(P_{n_e}^e + \left(1 - P_{n_e}^e\right)P_{n_p}^p\right)\right) \tag{25}$$

where t is the task solution time, $M_{n_r}^r$ is the mathematical expectation of the program operation delay time in case of n_r being the backup points, p is the SW error-free performance (SW efficiency), $P_{n_e}^e$ is the error prevention probability in case of n_e environment control points, and $P_{n_p}^p$ is the error detection probability in case of n_p SW control points.

In the above formula, p is the SW failure-free performance probability; error prevention probability—$P_n^e = (n_e + 1)\cdot F\hat{z}$; error detection probability—$P_n^p = \left(n_p + 1\right)\cdot F_{\hat{z}}$; availability factor $R' = \left(\frac{t}{\left(t+M^r_{n_r}\right)}\right)$; $M^r_{n_r} = t + (n_r + 1)M_{\hat{z}}$.

The constraining factor (Eq. (25)) is the SW dependability cost index defined as the cost of standard procedures:

$$C\left(n_e, n_p, n_r\right) = C_e\, n_e + C_p\, n_p + C_r\, n_r \tag{26}$$

where C_p is the cost of one SW error detection control event; C_e is the cost of one environment control event for error prevention; and C_r is the cost of setting one checkpoint.

The SW operation security management task comes down to optimizing the availability factor, with the constraining factor (Eq. (26)). The following two optimization tasks can be defined:

1. **Direct task:** Using partial redundancy of the number of standard procedures, ensure that the SW security index is at least equal to the specified index R_{rg}, with a minimum possible cost of standard procedures in general, that is

$$\min\left\{C\left(n_e, n_p, n_r\right) \middle|\, R\left(n_e, n_p, n_r\right) > R_{rg}\right\} \tag{27}$$

2. **Reverse task**: Using partial redundancy of the number of standard procedures, ensure that the cost of all standard procedures does not exceed the specified value C_{rg}, with a maximum possible SW reliability index, that is

$$\max\left\{R\left(n_e, n_p, n_r\right) \middle|\, C\left(n_e, n_p, n_r\right) < C_{rg}\right\} \tag{28}$$

4.1. Direct optimization task

Analysis (Eq. (25)) showed that R is a nondifferentiable monotone increasing function that is strictly convex upward.

In order to solve optimization tasks, therefore, it is advisable to employ sequential search methods.

Let us assume the value of incremental difference $\Delta R(, n_r)/\Delta C$ to be an enumeration criterion. Let us determine an enumeration step in accordance with the dichotomy rule. In this case, the computational scheme for solving the direct task can be presented as follows:

1. Define a set of initial values of the number of standard procedures:

   $\boldsymbol{N_o} = \{n_0^{\,i}, n_0^{\,j}, n_0^{\,k}\}$, where $i,j,k \in \{e,p,r\}$.

2. Calculate the initial value R:

   $R_0 = R(N_o)$.

3. If $R_0 > R_{rg}$, perform the following operations:

3.1. Find a set of search interval values

$\boldsymbol{L}_0 = \{\ L_0^i,\ L_0^j,\ L_0^k\}$, where $L_0^l = n_0^l$ - n_{lw}^l; n_{lw}^l is the lower boundary n^l.

3.2. Obtain the set of possible values of the number of standard procedures

$\boldsymbol{N}_1{}^i = \{n_1{}^i, n_0{}^j, n_0{}^k\}$, where $n_1{}^i = n_0{}^i - \|L_0{}^i/2.\|$

3.3. Find another set of values of the number of standard procedures

$\boldsymbol{N}_1 = N_1{}^i$, where i is the index of the standard procedure conforming to the minimization condition:

min(R_0 - $R(N_1{}^i)/(C^i\|L_0{}^i/2\|)$), where $i,j,k\ \epsilon\ \{e,p,r\}$.

4. If $R_0 < R_{rg}$, perform the following operations:

4.1. Find a set of search interval values

$\boldsymbol{L}_0 = \{\ L_0^i,\ L_0^j,\ L_0^k\}$, where $L_0^l = n_u^l$ - n_0^l; n_{u}^l is the upper boundary n^l.

4.2. Obtain three sets of possible values of the number of standard procedures

$\boldsymbol{N}_0{}^i = \{n_1{}^i, n_0{}^j, n_0{}^k\}$, where $n_1{}^i = n_0{}^i + \|L_0{}^i/2\|$.

4.3. Find another set of values of the number of standard procedures

$\boldsymbol{N}_1 = \boldsymbol{N}_1{}^i$, where i is the index of the standard procedure conforming to the maximization condition:

max($\mathrm{R}(N_1{}^i) - \mathrm{R}_0$ - /($C^i\|\mathrm{L}_0{}^i/2\|$)), where $i,j,k\ \epsilon\ \{e,p,r\}$.

5. Increase the iteration index

$\tau = \tau + 1$.

6. Calculate the value R

$R_\tau = R(N_\tau)$.

7. Find a set of search interval values

$\boldsymbol{L}_\tau = \{\ L_\tau^i, L_{\tau-1}^j, L_{\tau-1}^k\}$, where $L_\tau^i = \|L_{\tau+1}^i/2\|$.

8. If $R_0 > R_{rg}$, perform the following operations:

8.1. Obtain a set of possible values of the number of standard procedures

$\boldsymbol{N}_\tau{}^i = \{n_{\tau+1}{}^i, n_\tau{}^j, n_\tau{}^k\}$, where $n_{\tau+1}{}^i = n_\tau{}^i - \|L_\tau{}^i/2\|$.

8.2. Find another set of values of the number of standard procedures

$\boldsymbol{N}_\tau = \boldsymbol{N}_{\tau+1}{}^i$, where i is the index of the standard procedure conforming to the minimization condition:

min(R$_0$ - R($N_{\tau+1}{}^{i}$)/($C^i\|L^i_\tau/2\|$)), where *i,j,k* ϵ *{e,p,r}*.

If $N_{\tau+1} = N_{\tau-1}$, withdraw from the procedure.

9. Otherwise ($R_\tau < R_{rg}$), perform the following operations:

9.1. Obtain the set of possible values of the number of standard procedures:

$\boldsymbol{N}_{\tau+1}{}^{i}$ = {$n_{\tau+1}{}^{i}$,$n_\tau{}^{j}$, $n_\tau{}^{k}$}, where $n_{\tau+1}{}^{i} = n_\tau{}^{i} + \|L_\tau{}^{i}/2\|$.

9.2. Find another set of values of the number of standard procedures

$\boldsymbol{N}_{\tau+1} = \boldsymbol{N}_{\tau+1}{}^{i}$, where *i* is the index of the standard procedure conforming to the maximization condition:

max(R$\left(N_{\tau+1}{}^{i} - R_0\right)$/($C^i$ $\|L^i_\tau/2\|$)), where *i,j,k* ϵ *{e,p,r}*.

9.3. If $N_{\tau+1} = N_{\tau-1}$, record the value $R_{\tau+1}$ = R ($N_{\tau-1}$) and withdraw from the procedure.

10. Proceed to item 5.

The period of this computation scheme can be reduced as follows:

- by specifying the effective initial values, for example, by using personnel's experience (knowledge) or statistically accumulative tables;
- by reducing the calculation of standard procedure indices to their calculation only as per deterministic models. This is acceptable with a great number of standard procedures (more than 5–20) when stochastic models are less effective than deterministic ones.

4.2. Reverse optimization task

The reverse task can be solved using the branch-and-bound procedure. In this case, the computation scheme will be as follows:

1. Specify a cost-ordered set N of initial values of the number of standard procedures

$\boldsymbol{N}_\tau$= {$n_\tau{}^{1}$,$n_\tau{}^{2}$, $n_\tau{}^{3}$}, $C^1 \geq C^2 \geq C^3$,

which meets the normalization requirement:

$0 \leq C_{rq}$ - $\sum_{i=1}^{3}\left(\text{n}\, C^i\right) \leq C^i$; $i = \overline{1;3}$,

where τ is the ramification index;

2. Calculate the maximum value R by directed enumeration n^{2}at the fixed value $\text{n}^1 = \text{n}^1_\text{r}$ and the initial value $\text{n}^2 = \text{n}^2_\text{r}$:

$R(N_\tau) = \max(R \mid n^1 = n^1_\tau)$,

where N_τ meets the normalization requirement;

3. Calculate the maximum value R by directed enumeration n^{2}at the fixed value $\text{n}^1 = \text{n}^1_\tau + 1$ and the initial value $\text{n}^2 = \text{n}^2_\tau$:

$R(N_{\tau+1}) = \max(R \mid n^1 = n^1_\tau + 1)$,

where $N_{\tau+1}$ meets the normalization requirement;

4. Calculate the maximum value R by directed enumeration n^2 at the fixed value $n^1 = n^1_\tau - 1$ and the initial value $n^2 = n^2_\tau$:

   $R(N_{\tau-1}) = \max(R \mid n^1 = n^1_\tau - 1)$, where $N_{\tau-1}$ meets the normalization requirement;

5. If $R_\tau = \max(R_{\tau-1}, R_\tau, R_{\tau+1})$, withdraw from the computation scheme;
6. If $R_{\tau+1} = \max(R_{\tau-1}, R_\tau, R_{\tau+1})$, let $\tau = \tau + 1$, perform item 3 and proceed to item 5;
7. If $R_{\tau-1} = \max(R_{\tau-1}, R_\tau, R_{\tau+1})$, let $\tau = -1$ and proceed to item 4.

In practice, there may be a task of calculating indices not for the SW functional stability (dependability) system in general but for a part thereof (checkpoint or error prevention/detection mechanisms). This means a transition from multidimensional to unidimensional task interpretation, which helps substantially simplify computational procedures. Thus, solving a partial reverse optimization task boils down to a single calculation of a specific index when $n = C_{\text{rq}}/C$.

When solving a direct task, the effectiveness of the computation scheme can be additionally improved by adjusting the variable change interval, for example, by defining the next variable value in accordance with a distribution law, and so on.

5. Conclusion

Thus, in this section, we have considered stochastic and deterministic models of SW periodic monitoring and backup, which allow for time and computational/data resource constraints. Representing monitoring and backup points as a restricted Bernoulli's flow helps obtain random time intervals with the preset number thereof and, accordingly, allow for the effect of stochastic external factors on the system operation process.

Comparative analysis of stochastic and deterministic models showed the former's effectiveness with a small number of control and backup points. Therefore, when managing IS stability by numerical methods, it is possible to identify preferred models (stochastic, deterministic, or combined) which enhance IS functional stability. This gives an effect akin to introducing structure redundancy, that is, a special type of redundancy (stochastic), the use of which is unlikely to result in higher costs. The application of stochastic models in engineering systems can be facilitated by using a random-impulse generator that forms random-restricted Bernoulli's flows [11].

A similar approach was taken as a basis to solve the problem of efficiency assessment of the diagnostic mechanism for data array failures. Apart from the IS resource control and backup domain, the above-stated results can be of use in assessing the cost-effectiveness of control measures and mechanisms being implemented in various engineering and management systems. For better use of stochastic models, it is possible to use a random pulse generator (e.g., [14]).

Author details

Alexey Markov[1]*, Alexander Barabanov[2] and Valentin Tsirlov[2]

*Address all correspondence to: mail@cnpo.ru

1 Bauman Moscow State Technical University, Moscow, Russia

2 NPO Echelon, Moscow, Russia

References

[1] Bird L, Higgins D, editors. Good Practice Guidelines 2013—Global Edition: A Guide to Global Good Practice in Business Continuity. 3rd ed. The Business Continuity Institute; 2013. 115 p

[2] Engemann KJ, Henderson DM. Business Continuity and Risk Management: Essentials of Organizational Resilience. Rothstein Associates; 2011. 370 p

[3] Pompon R. IT Security Risk Control Management: An Audit Preparation Plan. 1st ed. Apress; 2016. p. 311

[4] Stewart JM, Chappie M, Gibson D. CISSP: Certified Information Systems Security Professional Study Guide. 7th ed. Sybex; 2015. p. 1104

[5] Cummings D. Dataflow-Based Rollback Recovery in Distributed and Multi-Core Systems: A Novel Software Approach for Building Highly Reliable Distributed and Multi-Core Systems. Müller: VDM Verlag Dr; 2009. 236 p

[6] Garcia E, Antsaklis PJ, Montestruque LA. Model-Based Control of Networked Systems. Cham: Birkhäuser; 2014. 382 p. DOI: 10.1007/978-3-319-07803-8

[7] Getta JR. Discovering irregular periodic patterns in audit data. In: 2016 2nd IEEE International Conference on Computer and Communications (ICCC); 14–17 October 2016; Chengdu, China: IEEE; 2016. 16867467. DOI: 10.1109/CompComm.2016.7924671

[8] Huai L, Qiushi L, Jianxin H, Tongzhou J. A novel fault-tolerant scheduling algorithm for periodic tasks of distributed control systems. In: 2009 Chinese Control and Decision Conference (CCDC '09); 17–19; June 2009; Guilin, China: IEEE; 2009. p. 1584–1588. DOI: 10.1109/CCDC.2009.5192227

[9] Kostogryzov A, Nistratov G, Nistratov A. Some applicable methods to analyze and optimize system processes in quality management. In: Aized T, editor. Total Quality Management and six Sigma. InTech; 2012 Chapter 7. DOI: 10.5772/46106. Available from: https://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management

[10] Yin JY, Guo G-C, Wu Y-X. A Hybrid Fault-Tolerant Scheduling Algorithm of Periodic and Aperiodic Real-Time Tasks to Partially Reconfigurable FPGAs. In: 2009 International

Workshop on Intelligent Systems and Applications (ISA 2009); 23–24 May 2009; Wuhan, China: IEEE; 2009. p. 1–5. DOI: 10.1109/IWISA.2009.5072624

[11] Markov AS, Kernozhitsky VA. Economically effective data bases diagnostics method. Advances in Modeling and Analysis B: Signals, Information, Data, Patterns. 1995;**33**(3):5-12

[12] Markov AS. Paradigma ogranichennogo stohasticheskogo kontrolya [paradigm of limited stochastic control]. Izvestiya Instituta inzhenernoy phiziki. 2012;**1**(23):15-19 (In Rus.)

[13] Ushakov IU. Probabilistic Reliability Models. Wiley; 2012. 248 p

[14] Random pulse generator. Patent SU 840856. USSR; 1981; G06F 1/02; Bull. 23