Structural redundancy as robustness assurance of complex geoengineering systems

Alina Dychko[1,*], *Igor* Yeremeyev[2], *Natalya* Remez[1], *Serhii* Kraychuk[3], and *Natalia* Ostapchuk[3]

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Energy Saving and Energy Management, 37 Peremohy Ave., Kyiv, 03056, Ukraine
[2]Taurida National V. I. Vernadsky University, 33 Ivana Kudri Str., Kyiv, 04000, Ukraine
[3]Rivne State University of Humanities, 12 Stepana Bandery Str., Rivne, 33000, Ukraine

Abstract. The present paper provides that robustness is the facility of complex computer-aided geoengineering systems of keeping its feature invariable along the certain period of time. The detecting of indications which testify that system is not responding adequately to input disturbances may be realized by: comparing real data on assembly output with number of reference artefacts which correspond to specific states of disturbances; comparing real data on assembly output with a normal reaction to the actual set of input signals. To increase the resilience of monitoring data of geoengineering system the majority principle and the Byzantine agreement method are used.

1 Robustness problem

Robustness [1–3] characterizes the complex computer-aided geoengineering systems (CCAS) facility of keeping its feature invariable along the specified time. After this time such characteristics may gradually deteriorate but with a decrease in quality of operation within predefined limits (by reducing dynamic and static accuracy, increasing response time, increasing transient intervals, reducing possible additional functions, performance/cost metrics, etc.).

Robustness study helps to understand better the characteristics of the complex systems, geoengineering, energy efficiency and building energy sustainability in particular [2]. It's used when there is a need for a functional layer to provide built-in protection to ensure that it is robust with respect to requests that are issued at instances that are incompatible with its current state and could therefore cause catastrophic system failure [3].

There are the following ways of robustness assurance: structural redundancy; procedural redundancy; informational redundancy; combination of the all or some of above mentioned redundancies.

Structural redundancy presumes the duplicating structures utilization while each of them is capable to realize all the necessary procedures and control actions inherent to CCAS. There are the following ways of using duplicating structures:

- Simultaneous functioning of the two (or three and more) structures (dynamic or "hot" backup) with their activity results analysis and the structure of fault occurred deactivating if the specifics of wrong operation is detected;
- One of structures is operating when the other one is in standby reserve and shall be activated only after the failure of the currently operating structure is detected.

Every of mentioned ways of duplicating has intrinsic preferences and limitations.

Redundancy is considering as an additional type of structural performance indicator that is defined as a measure of warning available prior to system catastrophe [4]. The redundancy can be evaluated and its quantification can be formulated with the help of characteristics of the geoengineering systems functions. For optimization of their operation it's important to control the effects of maintenance on lifetime functions and redundancy [4].

The existence of redundancy assists in enhancing the safety and reliability of a system in its intact state; and mitigating the sensitivity or vulnerability of the structure to localised damage under an accidental situation. To assure such characteristics of the systems it's possible to take into account various stages where redundant structures are involved in and to develop essential means of designing for redundancy which can readily be integrated into safety decision-making [5]. Such approach should be considered in underground and on-ground construction, in mining and the extraction of minerals, in the assessment of subsidence and subsidence of soil bases etc. Generalizing the problem of structural redundancy, it should be emphasized that it implies the introduction into the system of additional equipment, structured in such way that even in case of failure of a certain part of the equipment, the system will continue to function successfully [6, 8, 11]. All these need the reliable control of information, which is impossible without system reliability engineering and its predicting with reliability monitoring scheme under changing environmental conditions [7, 9-11].

[*] Corresponding author: aodi@ukr.net

2 Structural redundancy

The simplest example of structural redundancy is the hardware duplicating and use in standby reserve either in dynamic or "hot" backup. In the first variant the one hardware is operating but the second one is idle or on maintenance prevention. In the second variant the both hardware operate simultaneously and supplementary monitoring hardware analyzes the operation of both complexes and makes a decision about what complex generates the more reliable information [12]. Each mode has the positive and negative distinguishing features. For example, the duplicating structure with standby reserve is developed in such way that after predetermined time of operation t_{rsb} when the probability of trouble-free operation

$$R = e^{-\frac{t_{rsb}}{m}}\frac{1+t_{rsb}}{m}, \tag{1}$$

(where m – trouble-free life) exceeds a certain set threshold, it is realized the transition to operating reserve set and the operated hardware is put on prevention for a time t_{mp}, during which the troubleshooting operations are carry out. It is the essential fulfilment of the condition $t_{stb} > t_{mp}$ while the more $\Delta t = t_{stb} - t_{mp}$ then the system's fault-tolerance is better. If the operating complex fails the standby reserve complex should be activated (if the last one isn't on prevention). This duplication approach is easy-to-work and requires the minimum of redundant hardware. But in case of failure and the need to switch to a backup set it is a loss of time connected with procedures for switching units, which leads to loss share information. If the standby reserve complex is on maintenance prevention the information drop may even result in overall fault. Therefore in such a case when loss of information and temporary stoppage of CCAS functioning are intolerable the dynamic or "hot" backup is used. In this case probability of failure-free operation along the time t_{hb} is estimated as:

$$R = e^{-\frac{t_{hb}}{m}}\left(2e^{-\frac{t_{hb}}{m}}\right). \tag{2}$$

In the case of "hot" reservation the complementary hardware is demanded for state analysis of every complexes and decision making of which of the blocks provides more reliable information. This hardware should also be duplicated in order to ensure its trouble-free operation. Therefore this way of structure redundancy is characterized by surplus of the complementary hardware as compared with standby reserve. Fault tolerance property in this case is guaranteed along the shorter time interval that is $t_{hb} < t_{sbr}$. But along that interval no losses of information in its unexpected fault from operating hardware occurs.

The detecting of indications which testify that assembly (subsystem, geoengineering system) is not responding adequately to input signals or disturbances, i.e. that it is a some loss of stability, may be realized by:

- comparing real data on assembly output with number of reference artefacts which correspond to specific states of disturbances (for detecting the cause of stability loss);
- comparing real data on assembly output with a normal reaction to the actual set of input signals (to detect the fact of stability loss).

Incidentally the distribution of points of set Y_i^f, which characterizes the real output signal is compared with distribution of points of reference signal Y_i^e and the Euclidean metrics

$$D\left[Y_i^f, Y_j^e\right] = \sqrt{\sum_{i=1}^{N}\left(y_i^e - y_i^f\right)^2} \tag{3}$$

is estimated.

If $D[Y_i^f, Y_i^e] < |\delta|$, where δ – maximum acceptable deviation of the real pattern from reference, the assembly is considered as correct one or corresponding to certain reference artefact.

3 Procedure of imbalance identification in systems

The algorithm that implement the above operations is presented in Fig.1-*A* –Fig.1-*D* and the conceptual layout of subsystem for some devices mismatching detecting and adjusting their features – in Fig.2. The following abbreviation is used here: UID – unit for information distribution, which depending on identical duplicating units' y_1 and y_2 state and subsystem's mode of operation, feeds the information on both units' inputs (if the loss of stability is not detected), locks out the inputs of both units (if the loss of stability is detected and faulty unit is identified) or locks out input of faulty unit (while correction procedure of the wrong data has place); UAM – unit of alternative models of assembly for the events of routine situation (proper operation, distortions due to specific common causes); URS – unit (source) of reference signals for testing the nodes and performing procedures for correcting the characteristics of defective nodes; UIE – unit of information's evaluation (the fact of loss of stability detection, fault unit identification, the optimal model selection); MU – memory unit for intermediate results of evaluations and corrections saving; UFC – unit of feature correction which implements the correction calculations in nodal points and choice of interpolation polynomials for calculations correction in all the residuary points of unit features.

In addition besides of majorization for fault tolerance the Byzantine agreement approach is used, which differs in that degree of redundancy need not to be as uneven number.

4 Principles of the resilience increase

As mentioned above, the further development of the method of structural redundancy consists in the use of the majority principle, or the principle of voting, which requires the introduction of multiple redundancy of data processing facilities, where multiplicity is an odd number equal to "3" or higher than it. When using majorization, the probability of a system failure can be determined from the expression

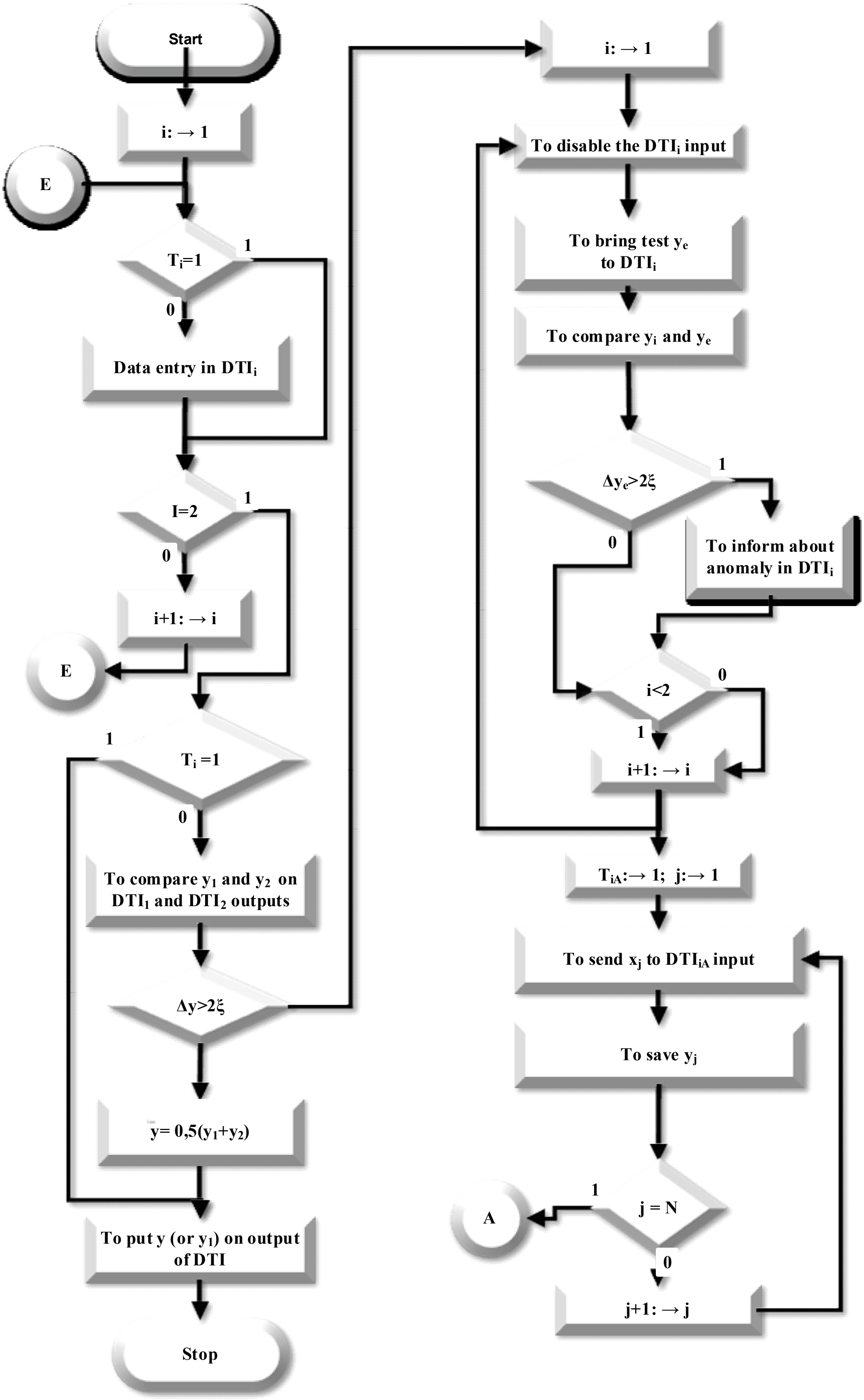
Start
i: → 1
E
T_i=1
1
0
Data entry in DTI_i
I=2
1
0
i+1: → i
E
1
T_i =1
0
To compare y_1 and y_2 on DTI_1 and DTI_2 outputs
Δy>2ξ
y= 0,5(y_1+y_2)
To put y (or y_1) on output of DTI
Stop
i: → 1
To disable the DTI_i input
To bring test y_e to DTI_i
To compare y_i and y_e
$Δy_e$>2ξ
1
0
To inform about anomaly in DTI_i
i<2
0
1
i+1: → i
T_{iA}:→ 1; j:→ 1
To send x_j to DTI_{iA} input
To save y_j
1
j = N
A
0
j+1: → j

Fig. 1. The block-diagram of algorithm of imbalance identification in homogeneous subsystems which duplicates one another (*A*).

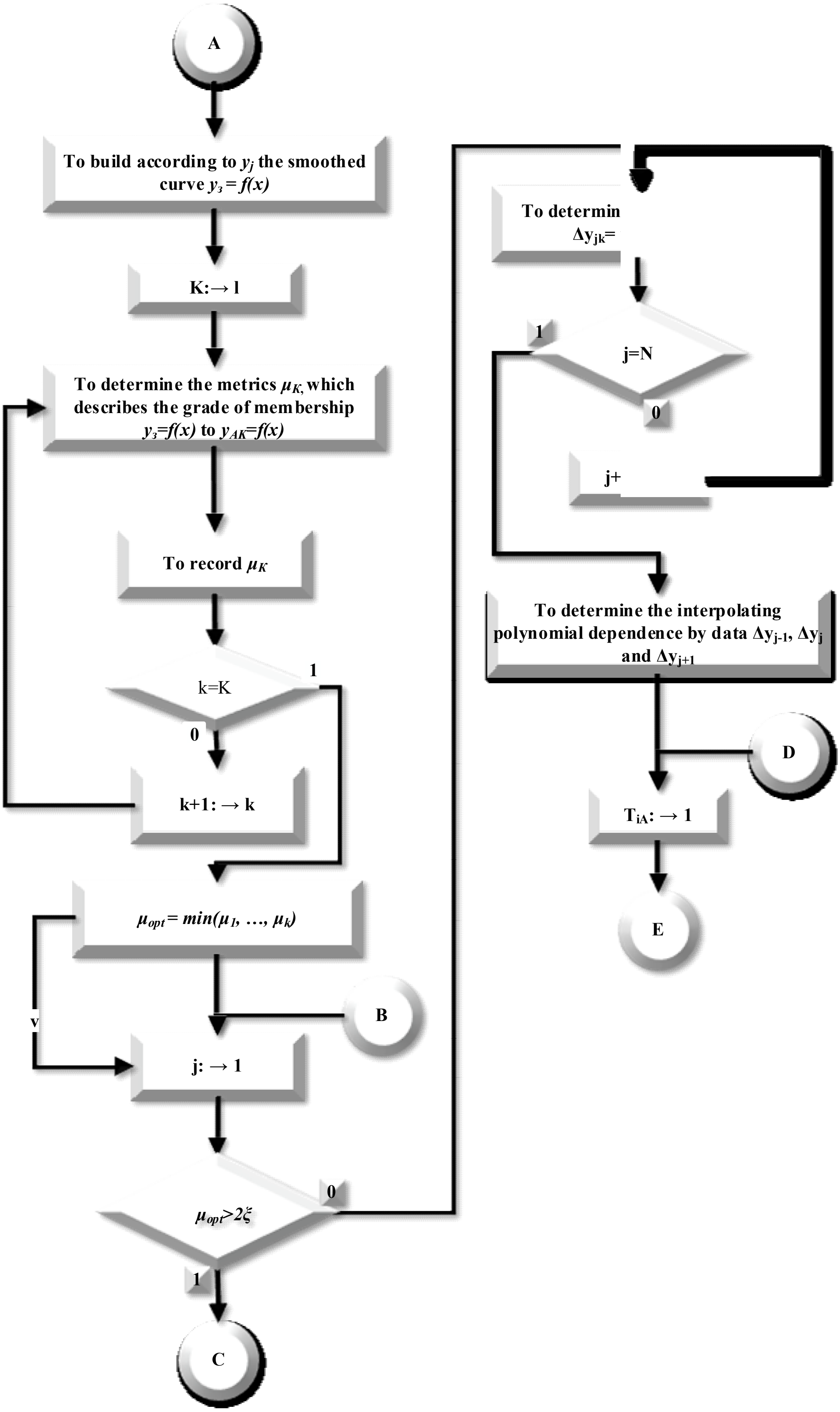
A
To build according to y_j the smoothed curve $y_з = f(x)$
K:→ 1
To determine the metrics μ_K, which describes the grade of membership $y_з=f(x)$ to $y_{AK}=f(x)$
To record μ_K
k=K
1
0
k+1: → k
$\mu_{opt} = min(\mu_1, \ldots, \mu_k)$
B
v
j: → 1
$\mu_{opt}>2\xi$
0
1
C
To determin
Δy_{jk}=
1
j=N
0
j+
To determine the interpolating polynomial dependence by data Δy_{j-1}, Δy_j and Δy_{j+1}
D
T_{iA}: → 1
E

Fig. 1. The block-diagram of algorithm of imbalance identification in homogeneous subsystems which duplicates one another (*B*).

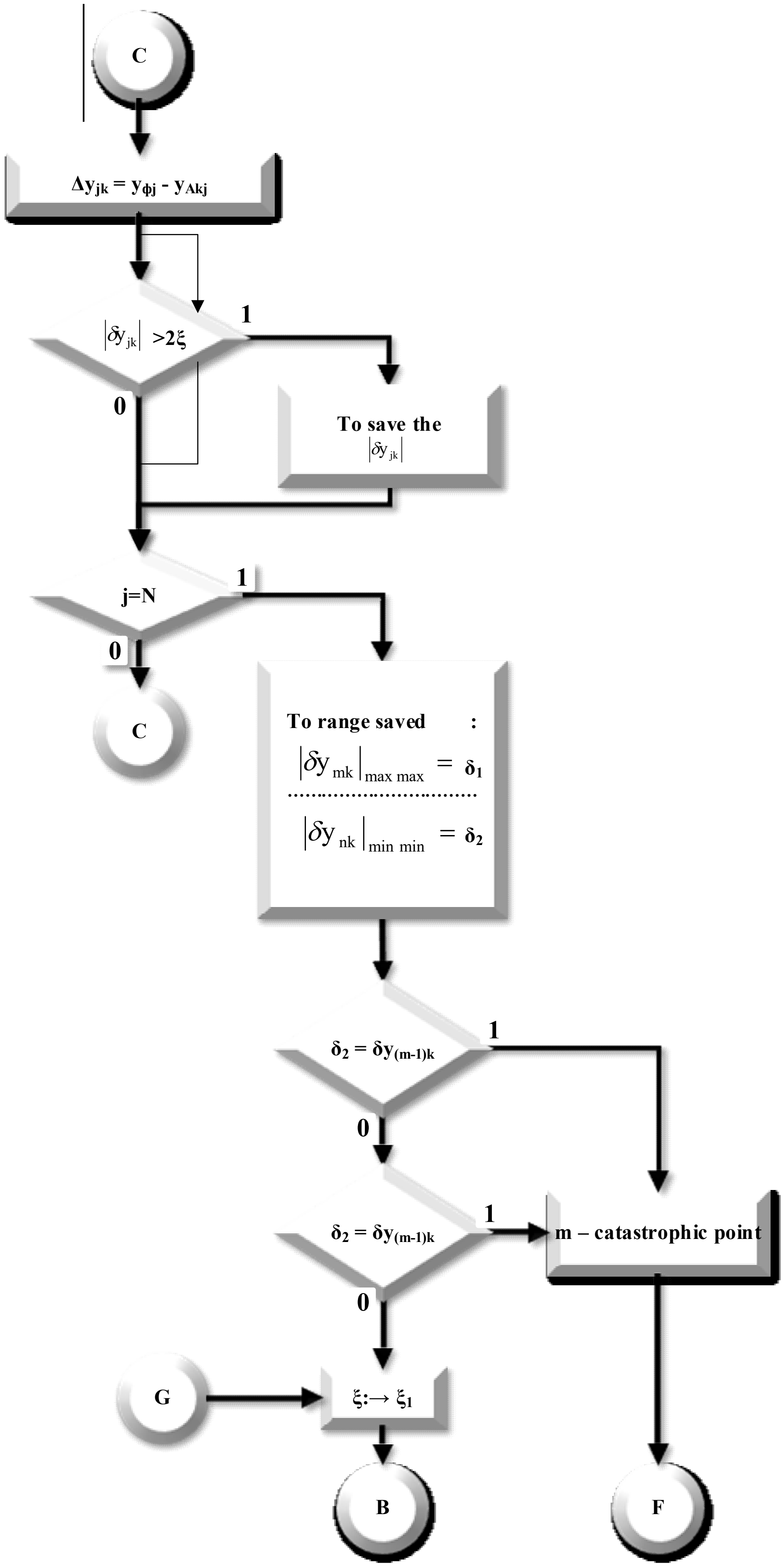
C
$\Delta y_{jk} = y_{\phi j} - y_{Akj}$
$|\delta y_{jk}| > 2\xi$
1
0
To save the $|\delta y_{jk}|$
j=N
1
0
C
To range saved :
$|\delta y_{mk}|_{\max\max} = \delta_1$
....
$|\delta y_{nk}|_{\min\min} = \delta_2$
$\delta_2 = \delta y_{(m-1)k}$
1
0
$\delta_2 = \delta y_{(m-1)k}$
1
m – catastrophic point
0
G
$\xi :\rightarrow \xi_1$
B
F

Fig. 1. The block-diagram of algorithm of imbalance identification in homogeneous subsystems which duplicates one another (*C*).

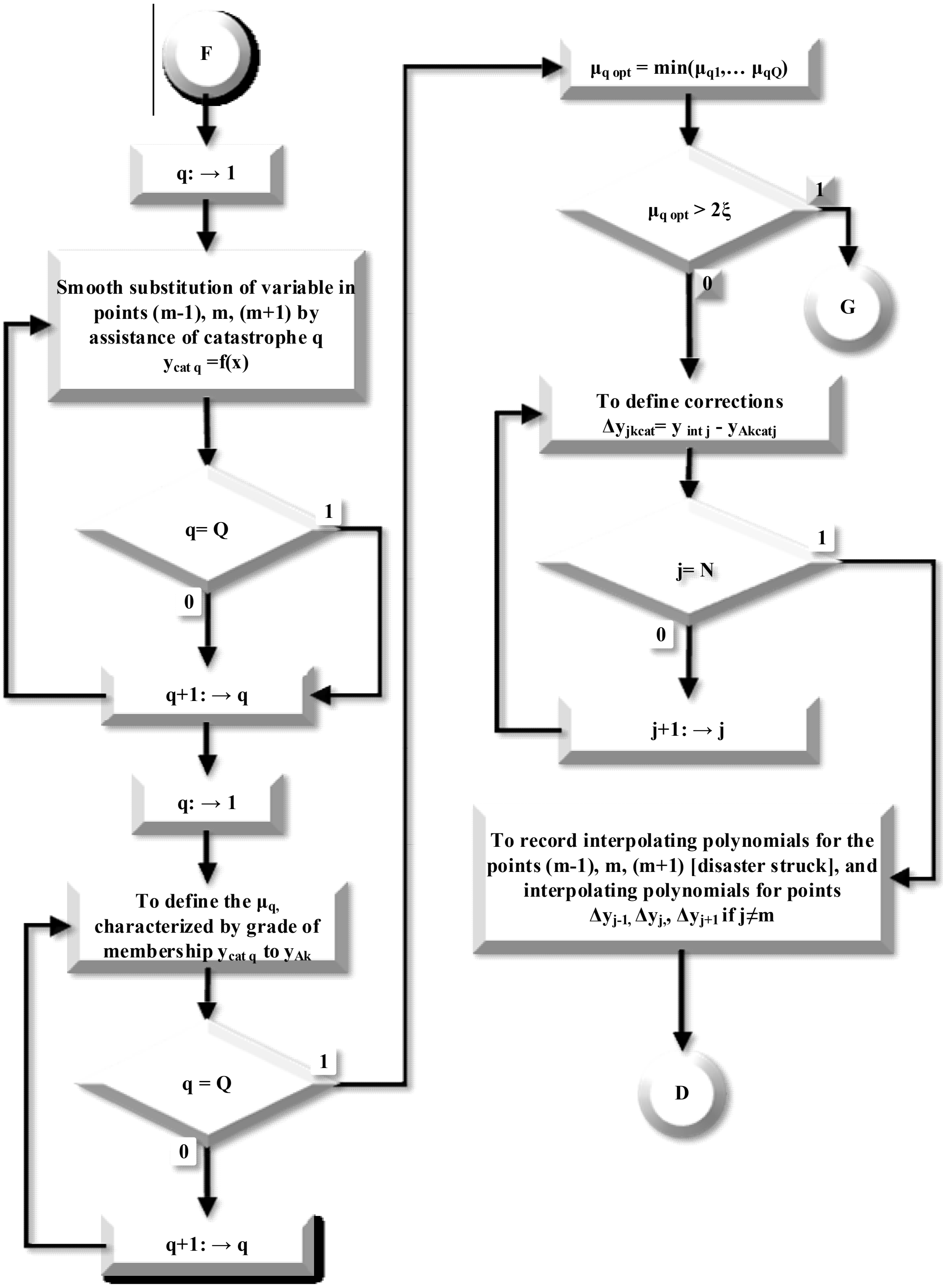
F
q: → 1
Smooth substitution of variable in points (m-1), m, (m+1) by assistance of catastrophe q
$y_{cat\,q}$ =f(x)
q= Q
1
0
q+1: → q
q: → 1
To define the μ_q, characterized by grade of membership $y_{cat\,q}$ to y_{Ak}
q = Q
1
0
q+1: → q
$\mu_{q\,opt}$ = min(μ_{q1},... μ_{qQ})
$\mu_{q\,opt}$ > 2ξ
1
0
G
To define corrections
Δy_{jkcat}= $y_{int\,j}$ - y_{Akcatj}
j= N
1
0
j+1: → j
To record interpolating polynomials for the points (m-1), m, (m+1) [disaster struck], and interpolating polynomials for points
Δy_{j-1}, Δy_{j}, Δy_{j+1} if j≠m
D

Fig. 1. The block-diagram of algorithm of imbalance identification in homogeneous subsystems which duplicates one another (*D*).

$$R_M = \left[\sum_{j=k}^{l} \binom{l}{j} R^l (1-R)^{l-j}\right]^n \qquad (4)$$

where *n* – number of sequentially connected blocks in the channel; *l* – number of channels, i.e. number of redundancies; *j* – number of properly operating channels (*j*≥ *k* , where *k* = { *l* / 2 } – the closest integer in excess of *l*/2; $R = e^{-t_{pM}/M}$ – probability of a single unit failing for time t_{pM} under failure conditions *M*.

Comparative characteristics of geoengineering systems using majorization principle with different redundancy values are given in Table 1.

In addition to the majority principle, the so-called "Byzantine agreement" is used to increase the resilience, characterized in that the multiplicity of redundancy is not necessarily characterized by an odd number. The formalism of the "Byzantine agreement" is effective when the total number of redundant (duplicate) blocks (duplication rate) is $n \geq 2\ k + m + 1$, where the blocks with failures are no more than *k* and *m* is the number of blocks that did not fail.

When using Byzantine agreement the denied blocks may remain connected with the system in any way and continue to function. It is only necessary to add that in such systems the source of the initial data is assumed to be quite reliable.

In a simpler case, such an approach should be that the result of the re-decision is compared with the first decision and if they are the same, the decision is recognized as valid and the control procedure is completed.

If the answer is different, a third repetition is initiated and if its result is equal to one of the previously obtained during the previous two steps of the decision, the answer is recognized as valid and the procedure ends. If, however, the decision obtained in the third step does not coincide with any obtained in the previous steps, a steady rejection signal may be issued. Sometimes a steady rejection signal can be provided after most 4…256 series solutions differ from each other by a value exceeding a predetermined threshold or double standard deviation.

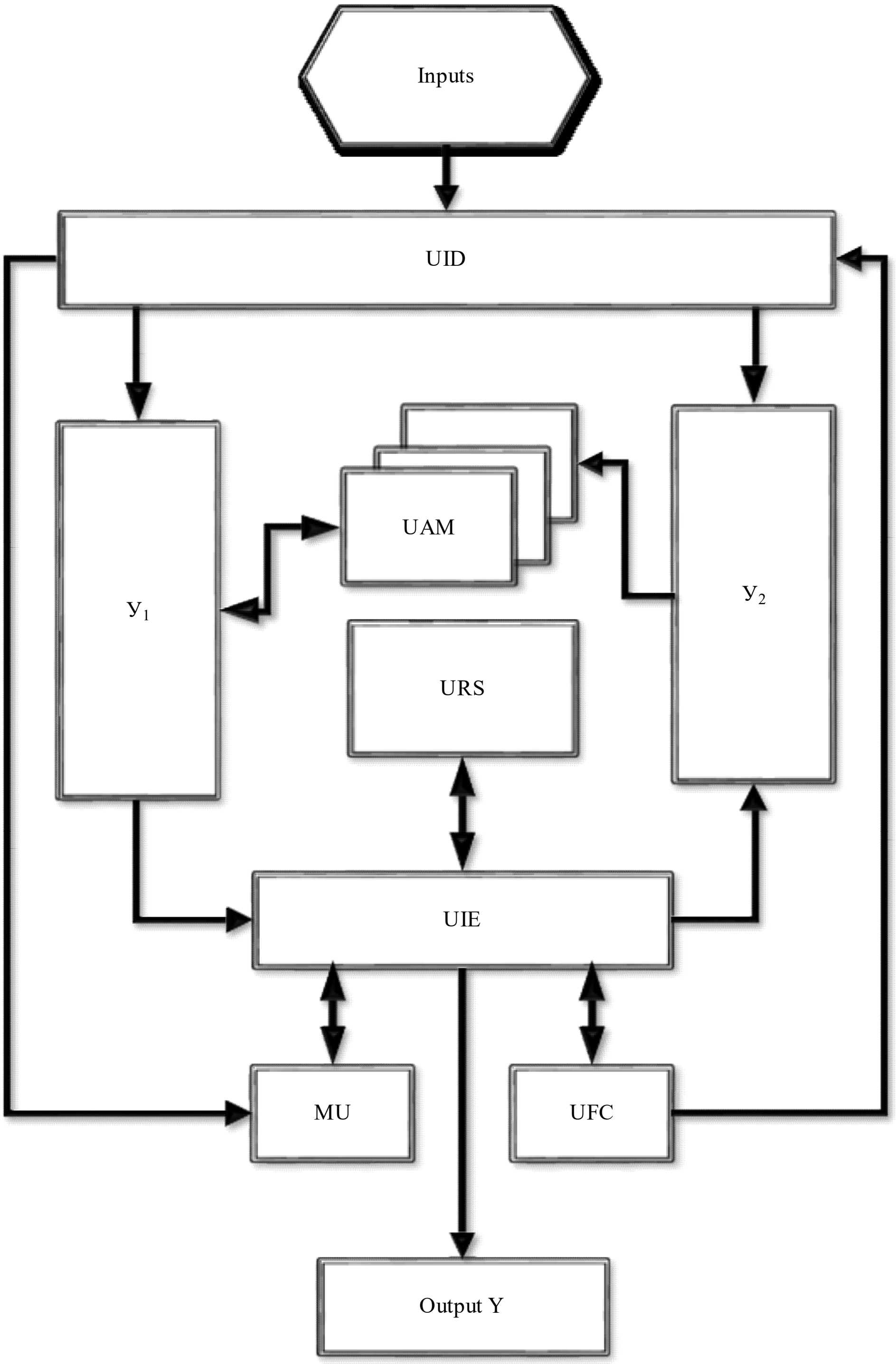

Fig. 2. Conceptual layout of subsystem for some devices mismatching detecting and adjusting their features

Table 1. Comparative characteristics of majorized systems with different meanings of redundancy rate.

Majorization	**Probability of no-failure operation RM**	**Probability of system output emergency (1–*RM*)**	
		R=0.9	R=0,99
2 from 3	$R_M = 3R^2 - 2R^3$	2.8x10^{-2}	3x10^{-4}
3 from 5	$R_M = 10R^3$ -15R^4 +6R^5	8.56x10^{-3}	1x10^{-5}
4 from 7	$R_M = 35R^4 - 84R^5 + 70R^6 - 20R^7$	2.73x10^{-3}	3x10^{-7}
5 from 9	R_M=125R^5-420R^6+540R^7-315R^8+70R^9	8.91x10^{-4}	1.3x10^{-8}
6 from 11	R_M=462R^6-1980R^7+3465RR^8-3080R^9+1386R^{10}-252R^{11}	2.96x10^{-4}	<10^{-9}

5 Conclusions

Robustness can be ensured by procedural redundancy, which implies a multiple solution by the same problem using the same source data, with the conclusion, that the outcome of the decision is correct, is based on the evaluation of most of the same (or close) decisions.

In case of using the “hot” backup duplicating system which contains a module that provides a comparison of the results of the solution of each of the autonomously operating complexes, the same results obtained at the outputs of both identical complexes prove their authenticity. If these outputs differ one from another it may be realized recurrent solution with the same input data, and solution results are compared with the results derived by every subsystem on preceding step. The same result obtained twice by the same complex is considered valid. The decision regarding the second subsystem is made on the basis of comparison of the second of the obtained decisions with a reliable result. If they are identical, the failure is considered unstable and the complex remains operating within the geoengineering system.

Otherwise, it is excluded from the operating circuit of the system and switched to the steady-state source diagnosis mode. The above procedures can be performed either autonomously or as part of a triple redundancy system with a majority principle of assurance. In the latter case, they provide additional stability of the geoengineering system in case of failure of one of the blocks of the system.

References

1. E. Cardinaels, *Job allocation in large-scale networks with locality constraints* (Eindhoven University of Technology, 2018)
2. V. Subouri, P. Femenias, in *Sustainability in energy and buildings* (Springer-Verlag, Berlin Heidelberg, 2013)
3. D. Powell et al., in *EDCC’12. Proceedings of the 2012 Ninth European Dependable Computing Conference*, IEEE Computer Society, USA, May 2012. doi: 10.1109/EDCC.2012.16
4. N.M. Okasha, D.M. Frangopol, Reliability Engineering and System Safety **95**, 5 (2010)
5. Z.X. Fang, H.T. Fan, Procedia Engineering **14**, (2011)
6. B.S. Dhillon, *Engineering maintenance: a modern approach* (CRC Press, 2002)
7. M. Ram, *Modeling and simulation based analysis in reliability engineering* (CRC Press, 2018)
8. I.H. Witten, E. Frank, M. Hall, *Data Mining. Practical Machine Learning Tools and Techniques*, 3rd edn (Morgan Kaufmann, 2011)
9. R.W. Scholz, *Environmental literacy in science and society: from knowledge to decisions* (Cambridge University Press, 2011)
10. G.A. Statiuha, Systems Proceedings and Information technologies **4** (2011)
11. A. Hinrichs et al., in *Dagstuhl Reports 2016*, **5**, 9 (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016)
12. A. Dychko, I.Yeremeyev, V. Kyselov, N.Remez, A.Kniazevych, Latvian Journal of Physics and Technical Sciences **6 (**2019)