Testing digital instruments and power systems devices

Pavel Pavlov[1,*], *Vladimir* Fandeev[2], *Valery* Butakov[1], *Dilyara* Baymeeva[1], and *Venera* Safiullina[1]

[1]Kazan State Power Engineering University, Kazan, Republic of Tatarstan, Russia
[2]Penza State University, Penza, Russia

Abstract. Discussed here is a technique for testing digital devices based on the calculation and control of two or more characteristics of a binary electric signal at a reference point. Signals coming from a healthy and failed digital device that are indistinguishable by the value of one of the characteristics may differ in value of the other characteristic. The combination of test methods can significantly reduce the potential of not detecting the failure of digital device. The technique is aimed at increasing the information content of the healthy state monitoring results and the possibility of localizing failures in digital instruments and devices of power systems.

Introduction

Comprehensive power systems consist of hardware that serves for various purposes and operate in different applications, including digital controls, monitoring and testing means. Such means include digital components of relay protection and automation (RPA) based on digital integrated circuits, microprocessor-based hardware components and microcomputers. The results of monitoring and testing ensure taking error-free decisions on safe operation and resource savings during the operation of hardware. Operational safety of equipment is provided by controls and testing tools, which are operated using hardware and software selected depending on the modes of operation, design and failure classes of devices being part of the I&C package.

Test check of a digital device by comparing the binary signal at the reference point with a valid binary signal guarantees the failure detection, but requires significant costs for testing support. Limiting the cost for testing support is achieved, for example, by selecting the number of transitions, the number of ones, and the signal signature at the reference point of the digital device as controlled parameters [1, 2]. However, the control of the number of transitions, the number of ones, and the signature is inferior to the method of comparing signals with the probability of failure detection.

Some failures failed to be detected by the signature control can be detected when the signature control and the number of transitions or/and ones of binary signals of the digital device are combined [3, 4]. The technique is aimed at determination of failures in the digital device and their number, which are not detected by one of the methods, but are detected by another or a set of other testing methods, as well as to assess the probability of not detecting a failure by each of the methods.

Testing models of digital device

The signal at the reference point of the digital device being tested is usually modeled as a multi-bit binary sequence of ones and zeros, which, in turn, is represented by a binary polynomial or Boolean function [1, 5, 6]. All three models make it possible to calculate the number of transitions, ones, and signal signature.

The number of different binary signal sequences is calculated by the formula

$$M = 2^N = 2^{2^n}, \tag{1}$$

where N is the number of bits of the binary sequence; n is the number of binary input signals (inputs) of the digital device.

A single valid binary sequence corresponds to a healthy digital device. The rest of the binary sequences correspond to failures of the digital device.

Combination of control of the number of transitions and the number of ones

The probability not to detect failure of the digital device by controlling the number of transitions or ones for equally probable binary sequences is calculated by the formula [1]

$$q = \frac{1}{M(M-1)} \sum_{k=0}^{N} C_N^k (C_N^k - 1) \approx \frac{1}{\sqrt{\pi N}}, \tag{2}$$

where k is the number of transitions or ones in the binary sequence; C_N^k is the number of combinations from N to k.

---

* Corresponding author: pavlov2510@mail.ru

The binary sequences of a healthy and failed digital device differ most often only in one bit (single failure). The probability not to detect single failure by controlling the number of transitions is calculated by the formula [1]

$$q_1 = \frac{N-1}{2N} \approx \frac{1}{2}. \quad (3)$$

A single failure can be detected by controlling the number of ones. Indeed, when changing 1 to 0 or 0 to 1 in a single bit, the number of ones in the binary sequence always changes. Thus, the control of the number of ones has an advantage over the control of the number of transitions in terms of detecting single failures.

The binary sequence of a failed digital device may not differ from the binary sequence of a healthy digital device in the number of transitions (ones), but it may differ in the number of ones (transitions). The corresponding failures of the digital device are not detected by controlling the number of transitions (ones), but can be detected by controlling the number of ones (transitions) [3].

The number of groups of binary sequences with the same number of transitions, but different number of ones, can not exceed the number of bits of the binary sequence:

$$G_{Nk} = 1, k = 0,$$
$$G_{Nk} = N-(k-1), k = 1,2,\ldots,N, \quad (4)$$

where G_{Nk} denotes the number of groups of N-bit binary sequences with the same number of transitions, but different number of ones.

The total number of groups of binary sequences with the same number of transitions, but different number of ones in the group is calculated by the formula

$$G_{Nk} = \sum_{k=1}^{N} [N-(k-1)] + 1. \quad (5)$$

The probability not to detect failure resulting from an N-bit binary sequence containing k transitions and l ones is calculated by the theoretically valid formula

$$Q_{k,l}^{N} = \frac{C_N^k (C_N^k - 1)}{M(M-1)} \sum_{l=1}^{N-1} \frac{M_{k,l}^{N} - 1}{C_N^k - 1}, \quad (6)$$

where $M_{k,l}^{N}$ is the number of N-bit binary sequences containing l ones among binary sequences containing k transitions (Table 1).

The probability not to detect failure when controlling the number of transitions and the number of ones is calculated by the formula

$$Q = \sum_{l=1}^{N-1} Q_{k,l}^{N}. \quad (7)$$

Table 1. Formulas for calculating the value $M_{k,l}^{N}$.

k	l	$M_{k,l}^{N}$
0	0	$M_{0,0}^{N} = 1$
0	$l \neq 0$	$M_{0,l}^{N} = 0$
1	$l = 1, 2, \ldots, N$	$M_{1,l}^{N} = 1$
2	$l = 1, 2, \ldots, N-1$	$M_{2,l}^{N} = N - l$
Odd, $k=N$	$l = N - \dfrac{k-1}{2}$	$M_{N,l}^{N} = 1$
Even, $k=N$	$l = N - \dfrac{k}{2}$	$M_{N,l}^{N} = 1$
Odd, $N>1$, $k<N$	$l = (k+1)/2$ to $N-(k-1)/2$	$M_{k,l}^{N} = M_{k-1,l-1}^{N-1} + M_{k,l-1}^{N-1}$
Even, $k<N$	$l = k/2$ to $N-k/2$	$M_{k,l}^{N} = M_{k-1,l}^{N-1} + M_{k,l}^{N-1}$

Fig. 1 is the ratio of probability values of not detecting the failure by controlling the number of transitions and ones and controlling only the number of transitions.
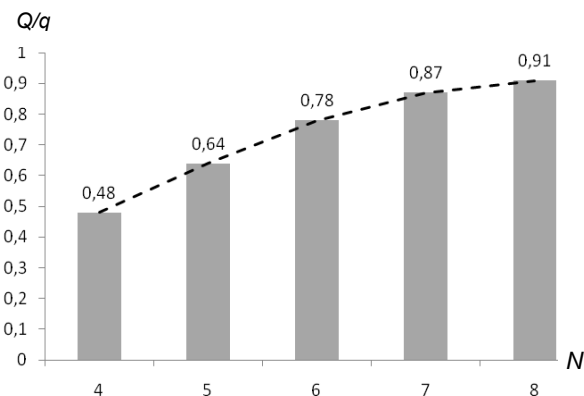

Fig. 1. The chart of the probability ratio not to detect failure by controlling the number of transitions and ones and controlling only the number of transitions.

As the number of bits in a binary sequence increases from four to eight, the probability not to detect failure by controlling the number of transitions and ones approaches the probability of not detecting the failure by controlling only the number of transitions. Controlling the number of transitions and ones does not significantly reduce the probability of not detecting the failure.

The combination of signature control and the number of ones

The probability not to detect failure of the digital device by signature control as calculated by the formula [7]

$$q_s = \frac{2^{N-m} - 1}{2^N - 1} \approx \frac{1}{2^m}, \quad (8)$$

where *m* is the number of bits in the signature analyzer register, it is many times less the probability not to detect failure by controlling the number of transitions and ones.

A significant reduction in the probability not to detect failure of the digital device is achieved by a combination of signature control and the number of ones. Actually, the calculation of the signature according to the rules justified in [5] shows that the binary signal sequences of a healthy and failed digital device may not differ in the signature, but may differ in the number of ones [8].

The probability not to detect failure by a combination of signature control and the number of signal ones is calculated by theoretically valid formulas for a signature containing one in at least one of the bits (non-zero signature, $s \neq 0$), and a signature containing zeros in all bits (zero signature, $s=0$):

$$q_{l,s \neq 0} = \frac{1}{M-1}\left(\frac{N-1}{N/2} \sum_{c=1}^{l/2} C_{N/2}^{2c-1} C_{N/2}^{l-(2c-1)} - 1 \right), \qquad (9)$$

$$q_{l,s=0} = \frac{1}{M-1}\left(C_N^l - \frac{N-1}{N/2} \sum_{c=1}^{l/2} C_{N/2}^{2c-1} C_{N/2}^{l-(2c-1)} - 1 \right), \qquad (10)$$

where M, N are calculated by the formula (1); l is the number of ones of the binary signal sequence, $l/2$ is rounded to the nearest integer for an odd number; C stands for the number of combinations; c is an integer variable.

The approximate probability not to detect failure of the digital device by a combination of signature control and the number of ones is calculated for nonzero and zero signatures by the formula

$$q_{l,s} \approx \frac{1}{M-1}\left[\frac{(N-1)!}{l!(N-l)!} - 1 \right], \qquad (11)$$

Formulas (9)-(11) are obtained for the number of bits of the signature analyzer register equal to the number of binary input signals (inputs) of a digital device. Probabilities (9)-(11) take maximum values for $l=N/2$. The accuracy of formulas is confirmed by the results of a computational experiment with binary sequences.

The maximum probability not to detect failure by a combination of signature control and the number of ones is significantly less than the probability not detect failure by controlling only the signature (Table 2).

Table 2. Probabilities not to detect failure by signature control, a signature, and the number of ones.

N	q_s	$q_{l,s}$	$q_{l,s}/q_s$
4	0.25	0.033	0.13
8	0.13	0.030	0.24
16	0.063	0.012	0.20
32	0.031	0.0044	0.14
64	0.016	0.0016	0.099
128	0.0078	0.00055	0.07

The decision regarding the failure of the digital device is made if the signal signature does not match the valid signature or the number of ones does not match the valid number of ones. The valid signature and the valid number of ones are calculated or determined experimentally. The ones counter can be part of the signature analyzer.

Conclusion

The ability to combine signature control and the number of signal ones at the reference point in order to detect failure of the digital device is one of the possible trade-offs between conflicting requirements to limit testing support costs and detect failures with a high probability. A relatively small increase in the cost of testing support can significantly reduce the probability not to detect failures of digital components of relay protection devices based on digital integrated circuits, microprocessor-based components and microcomputers [9, 10, 11]. As a result, the reliability of operation of digital components of relay protection devices and, generally, power systems increases.

References

1. G.B. Willams, Troubleshooting on microprocessor based system. Oxford: Pergamon Rress Ltd., (1984)
2. GOST R 53480 Industrial product dependability. Terms and definitions, Moscow: Standartinform, (2009)
3. Zh. A. Romanovich, V.A. Scriabin, V. P. Fandeev, B. V. Tsypin, Testing, repair and maintenance of control systems for household machines and appliances: textbook. Moscow: Dashkov and Co., a publishing and trading corporation, (2016)
4. P.P. Pavlov, R.G. Idiyatullin, R.S. Litvinenko, On the issue of assessing the reliability of the city's electric transport system // Bulletin of transport information, 5, 23–26 (2017)
5. V.N. Yarmolik, Analysis of signature testability of digital circuits // Automatics and telemechanics, 10, pp. 156-167, (1989)
6. V.P. Fandeyev, Technology and failure analysis tools for recovered electronic devices: monograph. Penza: Penza State University Press, 240, (2001)
7. G. Gordon, H. Nadig, Localization of malfunctions in microprocessor-based systems using hexadecimal key codes // Electronics, 5, 23-33, (1977)
8. V.P. Fandeev, Vyach.P. Fandeev, P.P. Pavlov, Methodological reliability of signature analysis and improving its performance // New information technologies in complex systems: abstract, 88, (1995)
9. A.E. Auhadeev, R.G. Idiyatullin, L.N. Kisneeva, P.P. Pavlov, R.S. Litvinenko, Identification of electric traction in the urban electric transport system, IOP Conference Series: Materials Science and Engineering, 1,(2019)
10. N.F. Kashapov, L.S., Sabitov, R.S. Litvinenko, A.E. Auhadeev, P.P. Pavlov, Consideration of the influence of the reliability of elements of the urban

electric transport system on its bandwidth, IOP Conference Series: Materials Science and Engineering, 1, (2019)

11. E.M. Khusnutdinova, G.R. Khamidullina, P.P. Pavlov, A.E. Aukhadeyev, R.S. Litvinenko, and A.N. Khusnutdinov, Training transport specialists based on a contemporary view of self-organization of sophisticated developing systems, IOP Conference Series: Materials Science and Engineering, 1, (2018)