THE METHOD OF CONSTRUCTING A TEST SEQUENCE FOR TECHNICAL CONDITION CONTROL OF DIGITAL DEVICES

ORCID ID: 0000-0001-8512-7446

Vitalii Savran
PhD, Senior researcher of the research department of military-technical and information researches of the research department of information-psychological, geoinformation, military-technical researches of the research center
Military Institute of Taras Shevchenko Kyiv National University
UKRAINE

It is known that modern digital devices, which are used in many electronic systems, are complex and versatile. They are widely used in various technical devices based on large and ultra-large scale integrated circuits and microprocessor integrated circuits. Such digital devices are created on new principles based on replaceable elements of the digital standard [1-2]. Therefore, ensuring their high efficiency, that is, the ability to perform functions with a quality not lower than the stated, is the main requirement for them.

It is known that one of the main components that determine the quality of digital devices is reliability. The reliability of digital devices depends on many factors. Troubleshooting of such faults should be carried out in such a way that it does not affect the quality of the tasks of the digital device. To determine the technical state of a digital device, technical diagnostics and functional diagnostics self-test facilities are used.

The results of the analysis of the existing automated systems of technical diagnostics showed the low quality of reliable determination of the technical condition of a digital device [3-4]. If a digital device fails, the technical diagnostics system determines the malfunction in the group of suspects in the inoperability of regular replaceable elements. Such a faulty group is replaced by a faulty one from the warehouse. And if there is a suspicion of inoperability – they are sent to the service center. Such actions lead to reduction of its readiness factor and an irrational use of the technical support system for electronic equipment. The existing methods of diagnosing a digital device in place are outdated. This is due to the fact that existing diagnostic methods require a large number of control points and diagnostic parameters [3-4]. However, the increase in the number of checkpoints and diagnostic parameters complicates the system of automated technical diagnostics and increases the time for detecting faulty replaceable elements. Therefore, the development of the method of constructing a test sequence for technical condition control of digital devices is an important task.

To build a test sequence, methods are used that are based on a step-by-step representation of a digital device in the form of a set of modules. Such a test sequence should determine the technical condition of digital devices within a reasonable time frame and with the required reliability. Each part of a schematic function that is implemented in a digital device module is represented as a graphical functional diagram. The development of a method of constructing a test sequence for technical condition control of digital devices is based on general conceptual approaches [1, 3]. At the same time, the characteristics inherent in the process of diagnosing digital
devices based on the advanced spectral energy-dynamic method were taken into account [4].

The main stages of the method of constructing a test sequence for technical condition control of digital devices are [5]:

1. The choice of diagnostic model that describes the object of control with the required level of detail.
2. The determination of initial sets of parameters, construction of test sequence.
3. The choice of the criterion by which it is necessary to optimize the developed test sequence.
4. The determination of quantitative indicators that determine the degree of compliance of the developed test sequence with the specified requirements.
5. According to the results of the analysis of the obtained quantitative indicators:
   5.1. In case of non-compliance of the developed test sequence with the specified requirements, the choice of a refined diagnostic model. Then repetition of items 2-5.
   5.2. In case of conformity of the developed test sequence to the set requirements of acceptance of the test sequence.

It was also established that the decomposition of digital devices in modulus should be based on the following principles:
- the diagnostic model should be adequate to the digital device and accurately reflect its operation;
- the number of modules should be such that, in the future, satisfactory quality is ensured within the allowable time for building and optimizing the test sequence with the existing level of "automation" of the method for constructing the test sequence.

These principles have been learned in the development of the construction the method of constructing a test sequence for technical condition control of digital devices.

In the form of a graphical block diagram is presented the schematic diagram of the selected functions in the first, second, third and fourth stages [5]. To check the technical condition of each function, an elementary test operation is built, which provides the construction in an automatic mode. In the presence of feedback in the digital device, the existence of input gates is possible, on which the circuit is self-excited. A sign of self-excitation is the replacement of the variable at the input of the feedback element on the same set more than twice.

Thus, the rupture of feedback is one of the requirements for controllability of a digital device. Such an operation, which is performed algorithmically or physically, turns a digital device into a simple (in terms of building tests) a scheme in which the conditions of self-excitation are not met. However, there is a wide range of digital devices in which this requirement is not met.

In this case, it is necessary to check the test sequence for the presence of input data sets that cause self-excitation of feedback circuits. Moreover, it should be noted that the self-excitation, "fading" over time, does not exceed the period of filing the elementary test act. It is important to control the parameters of the quasi-short-circuit current pulses in the power bus during the next test set. Therefore, we will consider inadmissible (forbidden) those test sets that cause self-excitation of the circuit, and do not stop for a time equal to the period of filing the elementary test act. Prohibited test kits are subject to selection by blocking when checking the digital device. Detection of forbidden sets and memorization of the corresponding clock numbers is carried out at the stage of factory tests of digital devices in the process of selecting the test sequence.
Thus, the complexity of modern digital devices necessitates a step-by-step synthesis of methods for constructing a rational test sequence. Creating more efficient test sequences allows this of constructing a test sequence for technical condition control of digital devices method, which is based on the step-by-step synthesis.

References:


USE OF MACHINE LEARNING TO IDENTIFY ANOMALIES IN CYBERATTACKS

ORCID ID: 0000-0002-1954-8493

Volodymyr Matiievskyi
Department of Information Technologies and Systems
Luhansk Taras Shevchenko National University
UKRAINE

The active expansion of the use of computer networks in any sphere of life, the use of the Internet of Things is accompanied by the emergence of new cyber threats to the information security of the individual citizen, enterprise, state. The number and quality of cyber threats is growing. According to Cisco's annual cybersecurity report:

Attackers bring malware to unprecedented levels of excellence and impact (cryptocurrency ransom, new distribution methods);

Attackers are increasingly able to evade detection and use cloud services and other technologies commonly used for legal purposes as weapons (using encrypted malicious network communication, triple the growth of encrypted web traffic used by malware; using control channels to operate. based on legal Internet services such as OneDrive or GitLab);

Attackers exploit security gaps, many of which are related to the expansion of the Internet of Things (IoT) and the use of cloud services (expanding the use of botnets based on IoT, operating unprotected and uncontrolled IoT devices).

Given the above, it is worth considering the possibility of automatic and / or semi-automatic detection of cyberattacks in a poorly structured data, while understanding that the delay in response can lead to significant losses.