Particular characteristics of today's microelectronics and matters of highly dependable and secure control systems design

Aleksei P. Kirpichnikov, *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia*
Stanislav N. Vasiliev, *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia*

Abstract. Aim. *Drawing the readers' attention to the growing number of industrial disasters, associated damage, increasing human casualties and the connection of this phenomenon with computer-based automation systems. The authors produce arguments regarding the requirement for design technology with extended security features in view of the multifold growth of abnormal natural and industrial effects. The paper describes and analyzes distinctive features of control systems of critical application facilities and consequences of disregarding additional inspection of circuitry and software. Of special note is the growing risk caused by the introduction of unmanned technologies and their mass application in railway and automotive transportation. The paper examines the problems of control systems resilience to faults and external actions depending on the used components. Statistics of industrial disasters are provided, their connection with the indicators of control systems instability is examined. A special emphasis is put on the distinctive features of today's microelectronic components and the effects of technological progress on the systems' interference immunity and fault rate. Of note is the growing number of hazardous failures in systems based on 0.13-μm and lower microcontrollers. A significant attention is given to the research of the distinctive features of modern chips, their layout, particularly of the main element of a control system, i.e. the microcontroller and digital signal processor, the influence of the external effects on the chip. The matters related to CMOS layout in microprocessor-based units are considered, the dependance is shown between the rising noise influence and migration to new CMOS technology. Attention is drawn to the requirement to train an appropriate class of specialists able to work with such systems who have not only software engineering skills, but also profound knowledge of physics, fundamentals of control systems design and their stability.* **Results.** *A comparative evaluation of stability of 0.5 μm and 130 nm CMOS stability has been conducted. The resultant difference in threshold power of interference is over 4000 times. It is noted that most developers who design software for such systems are mislead by the non-availability of any public information on the fault rate of processing elements from the manufacturing companies. By taking the dependability figures as the main parameter they misjudge the safety integrity level, as instead of the fault rate parameters they erroneously use the microchip's dependability figures provided by the manufacturer. Additionally, standard methods of improving the safety level used by developers (e.g. redundancy) often prove to be inefficient.* **Conclusions.** *Designing highly dependable and safe control systems must take into consideration the distinctive features of today's computer components given the fact that new generations of modern microchips due to their fault rate characteristics are often unusable in highly dependable system design. It appears to be of relevance improving existing standards and developing new ways of increasing the stability and safety of systems. Also noted is the requirement of maintaining the level of education and awareness of a wide community of developers who work with control systems in transportation, energy, industrial automation, weapon systems, etc. as regards the importance of ensuring the required level of functional safety.*

Keywords: *computer-based control systems, microelectronic hardware components, industrial disasters, faults, SIL, safety unit.*

For citation*: Kirpichnikov AP, Vasiliev SN. Particular characteristics of today's microelectronics and matters of highly dependable and secure control systems design. Dependability 2017;3: p. 10-16. DOI: 10.21683/1729-2646-2017-17-3-10-16*

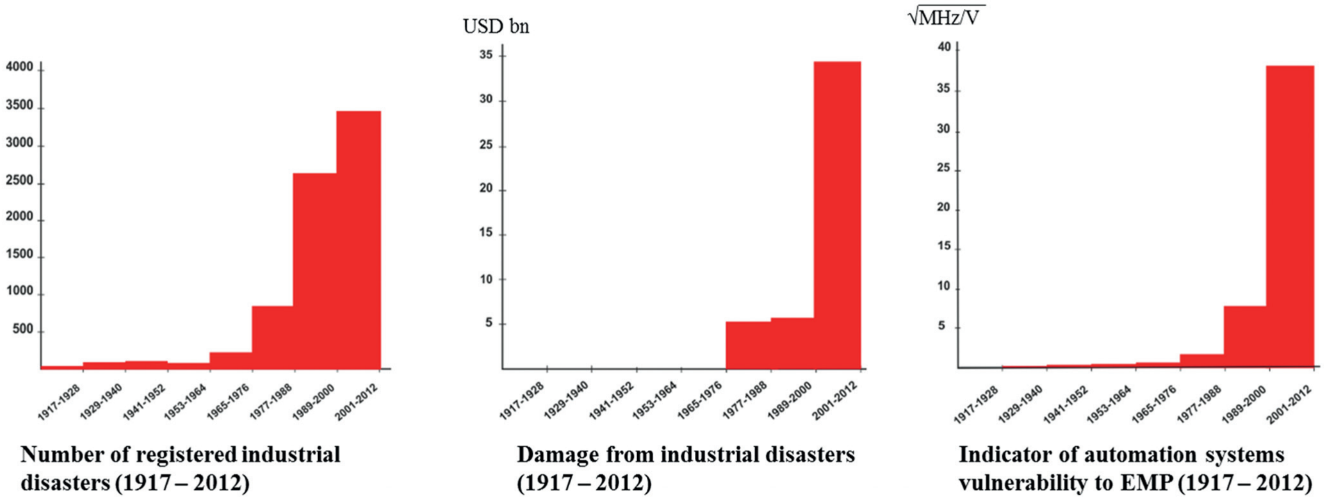
Introduction

The last few decades were marked by a menacing trend of constant growth of the number of industrial disasters that cause increasing damage and number of casualties. One of the primary reasons should be the general deployment of computer-control systems that replace old relay-based systems with no regard given to the specificity of the modern electronic components. The critical facilities control systems involve a very high level of safety that is practically unachievable with the new components without the use of very non-trivial methods. As the result, after modernization the facilities with the busiest operational schedules fall into the high risk group. Signal processing and safety systems design experts should pay special attention and be ready for very critical and intense work, which is not always typical for the modern times and unusual for the young generation. However, the result, i.e. saved human lives, is worth it. Therefore it is not recommended to leave such activities unattended, disregard additional inspection of circuitry and software (SW), on-receipt inspection of components and most importantly entrust the supply department with making decisions regarding alternative components. The consequences may be unpredictable and even tragic. The authors touched upon these aspects of safety in the context of railways and subways [1]. Moreover, for the teams of ICS RAS and OOO AVTEKS, the development of the BARS train control safety unit of 81-760 cars of the Moscow Metro was motivated by the ambition to counter the above mentioned trends.

It appears to be very important to achieve an adequate level of education and general awareness of a wide community of developers regarding functional safety. The requirement for extremely low probabilities of hazardous failures (e.g. 10^{-9} h^{-1} for SIL 4) makes the practical confirmation of the safety level by means of live testing of equipment practically impossible, which often pushes the matter into the realm of theoretical constructs and provides grounds for various legends and misunderstandings. Thus, a number of microcontroller and digital processor (DSP) manufacturers have announced new 90 nm and 65 nm SIL3 microchips with special error correction features. But all engineers know that microprocessors manufactured using old but still common 0.5 μm and 0.35 μm CMOS technology, provided there are no circuitry and layout design errors, de facto ensure fault rates as per SIL4 even under weak electromagnetic interference. Additional tests would improve those figures by two more orders of magnitude, which was rarely required in practice, when the matter was just in the failures due to dependability-related reasons. Modern 0.13 μm and lower microcontrollers and DSP, even given the embedded correction features in perfect laboratory conditions, are not always capable of complying even with SIL3 (10^{-7} h^{-1}) and in no case can be used in vital systems. This paper aims to at least partially clarify this matter.

Growth of the number of industrial disasters as the trend of the last decades

Let us start the examination with the industrial disasters. Their number (Figure 1) is obviously rising because it is proportional to the total number of technology units in use on the one hand and their growing contribution to the critical events on the other hand. The latter manifests itself both in the diversity of deployments (applications in facilities) and the variations of the step scale of consequences. As the result, we obtain a nonlinear (power) relationship. Despite the limited scale of the events, their effects are considerable and the specificity obvious: if supervision is disturbed (reliably operating safety systems are not in place) technology, especially energy-saturated, is elemental. The consequences of industrial disasters are locally always destructive, if only because technology (unlike volcanoes) is situated almost always near and among people. Of special significance in this



Number of registered industrial disasters (1917 – 2012)

Damage from industrial disasters (1917 – 2012)

Indicator of automation systems vulnerability to EMP (1917 – 2012)

Figure 1. Statistics of industrial disasters and changes in the automation systems stability

context is transportation and specifically railway and subway automation systems. Beside the regular risks the relentless progress (but in reality misunderstanding of the real situation and susceptibility to populism) dictates general deployment of automatics, unmanned technology, etc., which significantly increases the requirements for control systems and digital signal processing (DSP) units. Of special interest are the plans of mass deployment of unmanned automotive and air transportation (hopefully the GOST R IEC 61508 and ISO 26262 standards will not be disregarded in the process), which will have a significant impact on the safety of life.

Meanwhile, the statistics, even without those new and promising trends, look terrible. Let us take a look at the numbers, i.e. the statistics of industrial and natural disasters and their consequences over the last 100 years (based on data by the Centre for Research on the Epidemiology of Disasters, CRED) [2]. Thus, within 30 years between 1910 and 1940 (when the population of the Earth was about 2 bn people) the number of registered industrial disasters was just 162 and the number of people injured and killed was around 50 ths with the total damage amounting to about USD 102.5 mil. But within the same period between 1982 and 2012 (with the population of the Earth about 7 bn people) those numbers for the industrial disasters were about 6.7 ths with 4 mil people injured and killed and damage amounting to about USD 45.5 bn. In other words, the growth of the number of disasters was **35 times**, and **450 times** in terms of damage! The graphs shown in Figure 1 speak for themselves (for convenience, the data was processed with 12-year intervals, which is close to solar cycles on the one hand, and to the typical period of capital-intensive equipment modernization on the other hand).

Human thinking in population is characterized by delayed reaction (delay of one generation or more). On the one hand there is always «high-pass filtering» when small tactical events overshadow global trends, especially those where the time constant is more than several decades, and the generation develops a habit. That involves an adequate real-time reaction to current events from only a few professional communities at best, while the society at large ignores them.

How and by what means will the modern humanity try to react to the threat to its safety and the growing number of catastrophic events? Most probably with the same microprocessor-based protections, systems for information collection, processing and control. In this situation, we should be at least be concerned with purely professional matters of ensuring safety functionality, i.e. creation of technology that is capable to operate in adverse conditions when the probability of influencing factors abnormal in their magnitude grows multiple times. So, what is the typical resilience of automation systems to various effects (humidity, impacts, electromagnetic fields, etc.) and how was it changing over the past century? While in terms of mechanical strength and quality of manufacture the answer is obvious, the electromagnetic resilience must be evaluated. As the criterion let us take the conditional parameter of threshold effect that causes failure of such system [3, 4] measure it in units $V / \sqrt{MHz}$ in a similar way to noise spectral density. We omit intermediate calculations. The findings in the form of inverses are shown in the right-hand graph in Figure 1. A special attention should be given to the similar nature of the last two histograms: damage and instability of control systems.

Looking at the given graphs it becomes clear that standards must be overhauled and additional, non-market mechanisms of improving the stability of vital control systems must be discussed. Amidst the growing flow of catastrophe-inducing faults, «precedent» thinking with delayed reaction may fail. By taking that into consideration let us proceed to the examination of the specificity of modern microelectronic technology.

General problems of today’s microelectronic components

The list of components used n the control and safety systems is quite long and includes a large number of active an passive elements: from resistors, capacitors and transistors to large scale integrated circuits and radio frequency modules. Per each section of the list we should consider the effect of modernized technologies (most importantly nanotechnologies) on the dependability of components, their resilience to environmental effects and change of the probability of error associated with the performance of functions in the circuit. As the result, in particular, a new type of defect of surface mounted components was identified that is associated with mechanical effects in the process of manufacture and operation of products and lack of protection of surfaces of the modules that house the components. For most electronic modules we have a situation when the assembly guidelines have hardly changed in decades, yet the density of the layout has grown, the components stripped of casings (if those remained they were reduced to thin coatings that do not provide protection from mechanical damage), i.e. according to old standards most modern modules would be considered microassemblies and would require respective additional protection that is disregarded nowadays. Another uncovered factor was the changed nature of breakdown of active components which is primarily due to the use of low-voltage technology and significantly thinner layers in the structure of semiconductors compared to previous generations of similar products. We should also note the general application of power products based on MOS transistors, which on the one hand reduced the loss of power during switching, but on the other hand significantly increased the probability of breakdown of such switches to closure (due to the above mentioned problems of nanotechnology introduction). The list could go on as we discussed the impact of each factor on the safety and fault tolerance of control systems, but we shall confine ourselves to what we have said.

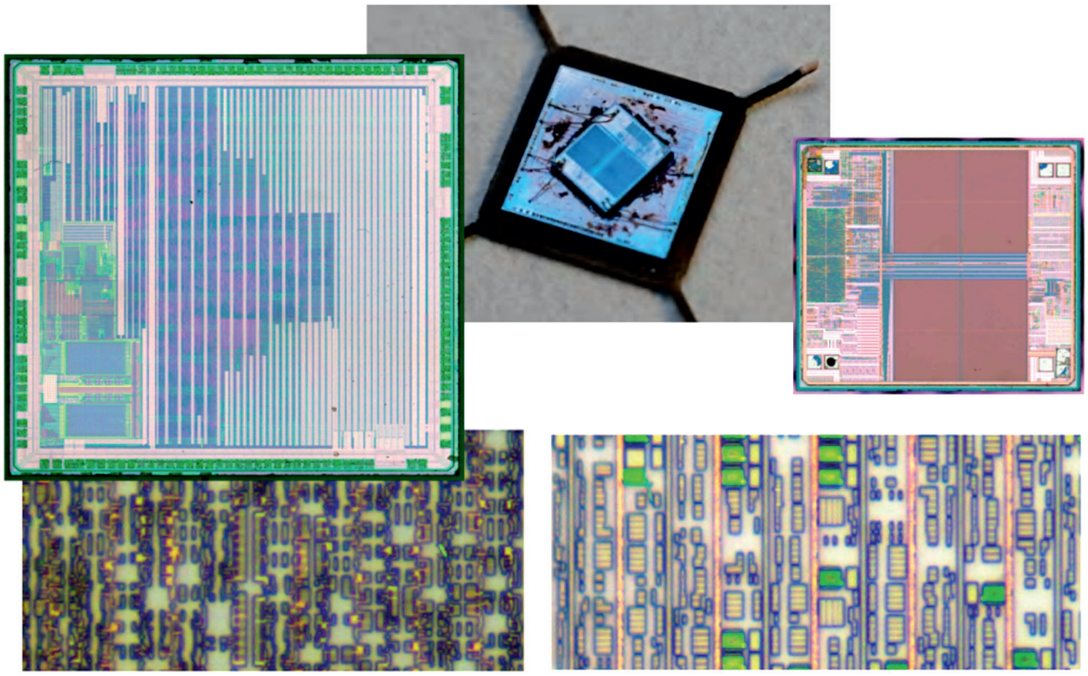


Figure 2. Cortex M3 microcontroller with the lid and pin matrix removed. On the left is a scaled image of a processor chip, on the right is FLASH memory, below, in more detail, are layout elements

Let us examine, even if briefly, the main element of a control system the processor unit (microcontroller, DSP, etc.) certainly is, the element on which depends the correctness of algorithm execution and safety of system's reactions.

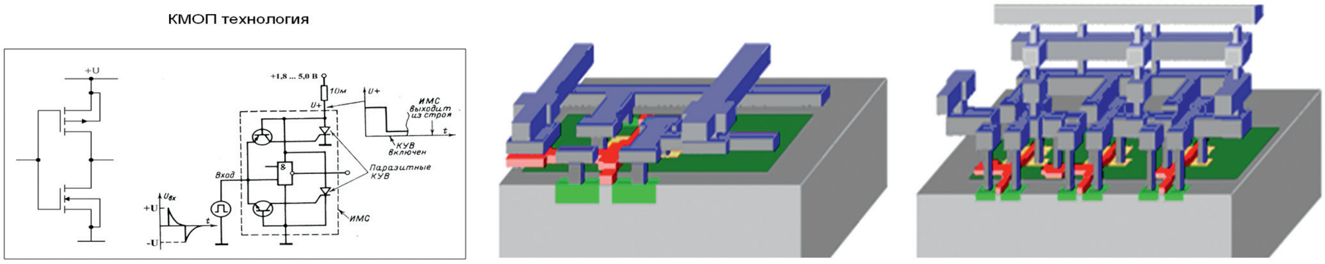
An example of such high technology component, that is well known but hardly recognizable in this form by IT experts, is shown in Figure 2.

Let us note that most developers who deal with system programming hardly understand what a microchip for which they design software is as an object in terms of physics and radio technology. As an example let us consider a popular Cortex M3-based processor, the successor to the well-proven ARM7. Figure 2 shows what such processor is without the case and the familiar pin matrix. Most importantly, we see not one, but two separate chips installed one on top of the other. The upper one is FLASH memory and is connected to the lower one (hardware core) with long links. The analysis of those connections immediately allows concluding on the difference in interference resistance of operations with RAM and FLASH due to those circuits alone. Other factors affecting the resilience will be the differences in chip technology, details of assembly, printed circuit boards (PCB), etc. However, our task does not consist in examining the features of a single component. Therefore let us, while briefly, touch upon the general problems of the CMOS technology one of the modifications of which is used in most modern microprocessor units.

Problems of the CMOS technology in modern microprocessor units

First of all, let us focus on a less popular fact: the CMOS logical gate, like any stage based on active elements at the moment of switching is an amplifier. For instance, in the case of an inverter (see diagram in the left-hand side of Figure 3) one transistor is the other one's load and the typical amplification ratio of such pair is usually around 80 – 100 in a broad band. In the right-hand part of the figure it is shown that this band changed from 90 MHz to 1.5 GHz with the transition from 0.5 µm to 0.13 µm. It should be taken into consideration that the threshold voltage and power supply of the transistors for the new technology is at least 4 times lower. That means that noise energy can be received by the circuit manufactured using the technology shown in the right-hand side part of Figure 3 from a band 16 times broader, given that its resilience to noise amplitude is at least 4 times lower.

While omitting intermediate calculations we note that the interference resistance of the currently used CMOS modifications with various design rules of external energy effects differs by orders of magnitude. The comparative evaluation of the **0.5 µm** and **0.13 µm** versions shown in the figure we obtain the value of the influencing interference that is different more than **4000** times **(!)**. The comparison of resilience for **0.5 µm** and **90 nm** shows the non-linear nature of this dependence, while the result of calculation is already over **15 000** times, all that is against the new chips that are so convenient for the users and software designers. That makes one wonder about the applicability of technology below 0.25 µm in critical application devices. It should be taken into consideration that the level of electromagnetic interference in modern civilization is very high in public places and energy-saturated infrastructure facilities. Thus, the operation of every safety device that is not resilient enough becomes a game of roulette.



Logic gate CMOS

0.5 μm, 2 layers of metal, up to 200K transistors, 90 MHz

0.13 μm , 7 layers of metal, up to 500 mil transistors, 1.5 GHz

Figure 3. CMOS technology: different density of metal layers and gates bandwidth for 0.5 and 0.13 μm

Having briefly considered the influence of environmental factors let us address the internal factors (i.e. those hidden within the microelectronic devices themselves). If in the context of previous generations of microprocessor devices the effect of radiation on the chip caused by ceramic elements of the case that with finite probability induced faulty switching of the chip's gates was discussed as a significant factor, now the definitively dominant effect is the poor magnetic compatibility of the densely situated elements and units of the chip itself, as we can see in Figures 2 (below) and 3. The factor of growing fault rate is the close location of the active elements and dense multilayer connections with the effect of crosstalk. It should be noted that for most modern processors the maximum length of a connection in the chip is 1 cm and more, which is also times more than the typical length of connection for the previous generation of circuitry.

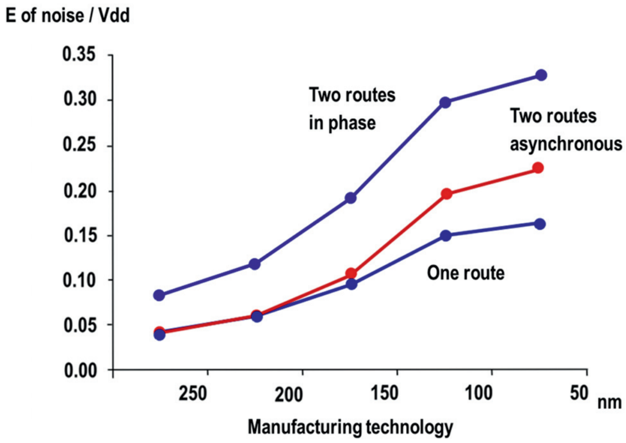


Figure 4. Dependence of the relative value of disturbance voltage on supply rail on the 1 mm-long routes

Figure 4 shows the dependence of the relative value of disturbing voltage in the power rail from 1-mm fragments of routes under topologically minimal distance between them as per design rules. The upper curve: signal in the source of interference changes in phase, middle curve: asynchronously, lowed curve: only one conductor with interference exists. Having taken into consideration the actual number of closely spaced routes on the chip and their lengths and having calculated the probability of peak values for the chosen noise model we obtain the approximate number of gate switching threshold overruns and an estimate of the fault rate of a specific microprocessor architecture (naturally, with no regard for the error compensation). Even this rough two-dimensional model yields results that are hardly compatible with the safety requirements. The results of 3D modelling of individual fragments of circuitry provide even more discouraging results. Additionally, large chips display a significant growth of loss current as an extra destabilizing factor that also indirectly influences the probability of faults.

That caused the interference resistance to fall and the fault rate to rise so much that it became noticeable in simple real-time systems (not safety-critical). The manufacturers were forced to use special fault compensation measures, i.e.: data surveillance and error correction units embedded in the chip, vital signals redundancy, etc. As the result, 65-nm chips with guaranteed SIL2 have appeared (NB, provided EMC in the equipment is perfect!). In other words, this has nothing to do with functional safety, as for products like that it counts as an achievement if some structures on one chip do not interfere too much with each other and can operate well under the fault rate of 10^{-6} h^{-1}. But that is absolutely not enough to build with their use even SIL2 safety system. Among the factors that radically affect safety will, for instance, be any electromagnetic effect with an appropriate probability of peak level within the considered time interval.

The usual practice of redundancy as a way to improve safety for such units also turns out to be not very effective due to fundamental reasons: under this technology, most faults [8] are common cause failure (CCF). Thus, even a low-power external electromagnetic effect that matches the frequency spectrum of a module's chips and connections "antennas" causes avalanching faults that cannot be mitigated with standard means of error correction that are designed to deal with non-numerous or isolated events. An effect threshold of sorts emerges, when the system's behavior becomes unpredictable. In case of safety systems it should be deemed absolutely intolerable and such components unusable. Their use must be confined to consumer and telecommunication devices, where the fault rate defines the availability of service and signal quality, but is in no way related with the safety of life.

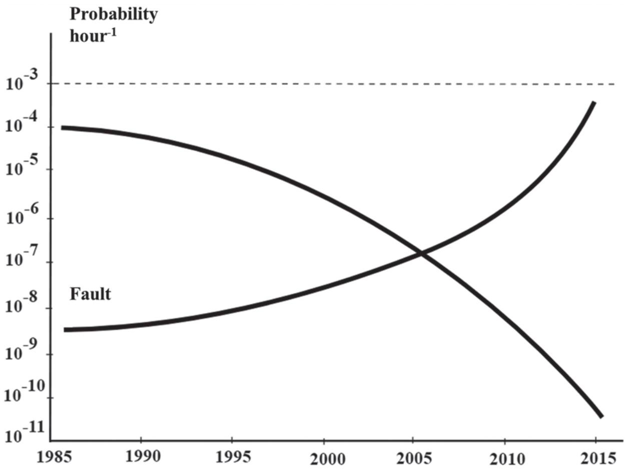


Figure 5. Evolution of the correlation between the failure probability and fault probability in microprocessor generations

As a result we have an unusual situation (Figure 5) when the dependability of microelectronic components is many times higher than their fault rate. So virtually the least dependable component of today’s electronic module is the PCB and connections, while the least unsafe is the processor element and sensitive digital circuits. In terms of fault rate, the most advanced electronics have achieved the level typical to human operators (i.e. we have achieved perfection and reproduced ourselves!). Fault rate data for most processor elements is not available in standard documentation and can be obtained only after long and tiring negotiations with the manufacturer (if it even bothers with testing the products and obtain such data). As the result, the developers while evaluating the safety integrity level (SIL) erroneously use the microchip’s dependability figures provided by the manufacturer instead, which is absolutely incorrect. As to the fault rate numbers, the information is confidential and is not discussed by the manufacturer.

This situation has a host of consequences. For instance, the replacement of a microcontroller with a newer version and fully SW-compatible can radically change the product’s SIL. Additionally, beside the processors there are additional interface circuits, analog-to-digital converters, clock speed generator and other microchips that contain digital modules manufactured using the technology the developer is not aware of that have their own fault rate numbers. Some of those faults can be mitigated algorithmically by the processor itself. But what can be done if the source of the fault is a phase jump of the reference signal, that causes totally uncontrollable consequences for digital systems? That can happen during a simple replacement of one component (a generator) in the specification with another one that is identical in terms of appearance and specifications (e.g. upon the supply departments’ advice).

Figure 6, as an example, shows five surface mounted board (SMB) generators of uniform application, i.e. intended for the same device, but by different manufacturers. Next are shown the results of “dissection” after the removal of the resonator. We can see digital circuits with totally different layout solutions, while the way the chip is assembled subsequently implies radically different interference resistance.

In conclusion, let us note that the development of microprocessors for SIL3 and let alone SIL4 control systems is hardly an easy task, especially for today’s design teams. Those teams are mostly composed of IT experts, who tend to disregard the physical and even radio technical effects in their work. This may prove to be fatal in the case of critical application devices and safety-critical applications...

References

1. Vasiliev SN, Kirpichnikov AP, Botvinionok AA. Problemi obespechenia bezopasnosti v sovremennykh mikroprotsessornykh sistemakh oupravlenia podviznym sostavom, vyzvannye osobennostiami sovremennoy elementnoy bazy, i ikh reshenie na primere bloka bezopasnosty “BARS” vagonov 81-760 Moskovskogo metropilitena [Challenges of ensuring safety in today’s computer-based train control systems caused by the specifics of modern computer components and their solution as in the case of the BARS safety unit of 81-760 cars of the Moscow Metro]. Bulletin of the JSC RZD Joint Academic Board 5:13–25 [in Russian].

2. Centre for Research on the Epidemiology of Disasters (CRED) <www.emdat.be>.

3. Kirpichnikov AP. Voprosy otkazoustoychivosty i bezopasnosty v oustroystvakh TsOS kriticheskikh prilozheniy [Matters of fault tolerance and safety in CSP devices of critical applications]. In: Proceedings of the Fourteenth

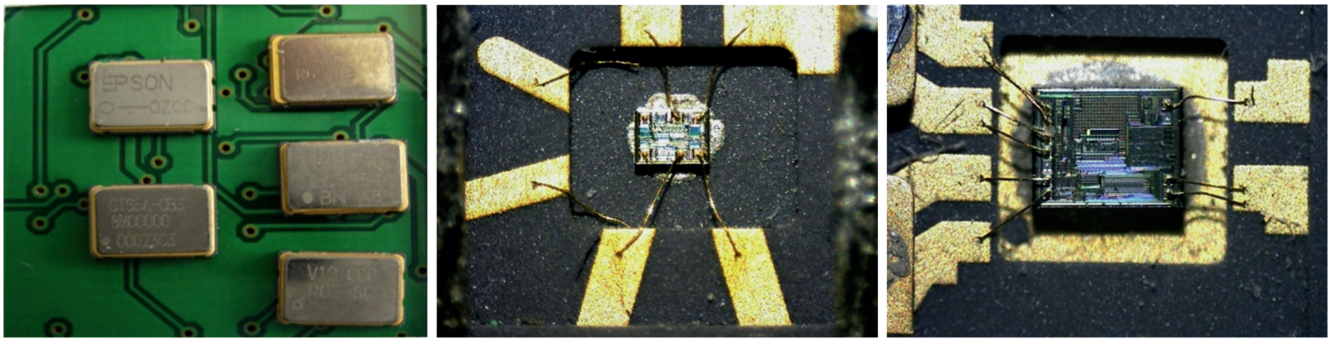


Figure 6. Interference resistance of MD generators Left to right: generators in cases SMD (5 types); low interference resistance version version acceptable in terms of process engineering and design

International Conference Digital Signal Processing and its Applications. Volume 1. Moscow (Russia); 2017. p. III–V [in Russian].

4. Kirpichnikov AP. Novaiya rol mikroprotsessornykh system: obespechenie bezopasnosti pered litsom katastrof [The new role of computer-based systems: ensuring safety in the face of catastrophes]. In: Proceedings of the Sixteenth International Conference Digital Signal Processing and its Applications, DSPA-2014. Volume 1. Moscow (Russia); 2014. p. 25-29 [in Russian].

5. Patent No. 2439666 RF. Kirpichnikov AP. Safety unit with validity checking of input information, 2010.

6. Patent No. 2449900 RF. Kirpichnikov AP. Safety unit, 2010.

7. Kirpichnikov AP, Botvinionok AA, Medunitsin NB. Mnogokanalnaya mikroprotsessornaya systema oupravleniya so sverkhvysokoy bezopasnostiu dlia poiezdov Moskovskogo metropolitena [Multichannel computer-based control system with ultrahigh dependability for the Moscow Metro trains]. Datchiki i sistemy 2014;9:38-45 [in Russian].

8. Shubinsky IB. Funksionalnaya nadiozhnost infromatsyonnykh sistem [Functional dependability of information systems]. Moscow: Nadiozhnost; 2012 [in Russian].

About the authors

Aleksei P. Kirpichnikov, head of unit, V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Russia, Moscow, phone: +7 (495) 334 89 10, e-mail: abramo@ipu.ru

Stanislav N. Vasiliev, member, RAS, Doctor of Physics and Mathematics, Chief Researcher, V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Russia, Moscow, phone: +7 (495) 334 89 10, e-mail: snv@ipu.ru

Received on 20.03.2017