TRANSBALTICA 2011

The 7th International Conference
May 5–6, 2011, Vilnius, Lithuania
Selected papers

ISSN 2029-2376 print / ISSN 2029-2384 online
ISBN 978-9955-28-840-4
http://transbaltica.vgtu.ltt

Vilnius Gediminas Technical University Transport Engineering Faculty, J. Basanavičiaus g. 28, LT-03224, Vilnius, Lithuania

AUTOMATIC DEVICE WITH FAULT TOLERANCE

Mareks Mezitis[1], Vladimirs Karevs[2]

Riga Technical University (Riga, Latvia), Riga Technical University (Riga, Latvia)
E-mail: [1]marek@dzti.edu.lv, [2]vladimirs.karevs@ldz.lv

Abstract. This paper considers the realizing examples for automatic device with fault tolerance. The most important device structures with and no reservation are compared.

The most common ways to increase fault tolerance are considered. The device structures with duplication and optimal are introduced.

The construction structures with redundancy and build in testing equipment BITE.

We consider fault tolerance in systems of high risk of sudden failure. A comparison of economic composes in the recovery efficiency of devices.

Proposed building for devices with high availability operating conditions with the inevitable risk of harmful effects.

We consider the probabilistic assessment of fault tolerance on each occasion.

Keywords: automatic device, duplication, redundancy, fault tolerance, sudden failure, risk of hazardous

1. Introduction

The requirements of safety and fault tolerance are required during the construction of automatics systems, subsystems or devices. Construction is selected depending on designation, usable function and location of action but must ensure safe continuation or completion of the control procedures, reliable information processing in cases, when number of the elements is in full or in part damaged.

Damage – violation of normal operation, caused by a change in the conditions of functioning with which in the elements occurs destruction or the violation of the physical plan of components is evinced by complete or partial loss by the element of basic functions.

The advantage of system, subsystem or device to “normal” function in this situation makes device fault tolerated.

The constructions of fault tolerated or resistant devices are based on use of component redundancy when the means of the determination of the state of components are present.

In certain cases the requirement of safety is the retention “normal” functioning even of the damaged device (masking of damage), in other cases switching into the safety state (controlled failure). By different authors and in different sources are examined the approaches of the construction of failure-resistant devices (1, 2, 3). There it is possible to find the estimated MTTF mean time to fault, fault rates and other parameters of the theory of reliability correspondently.

Statistical data more precisely describe object, if prolonged time is observed object and the greater the quantity of objects is observed. The most reliable result is obtained at the moment when it elapses the time of life of object or objects.

Trivial situations are it should be noted that by the authors examined.

For example in the device with majority decision making – voter is assumed to be the absolutely reliable (fig. 1). The voter in actual is device also has failure tolerated or resistant construction, etc.

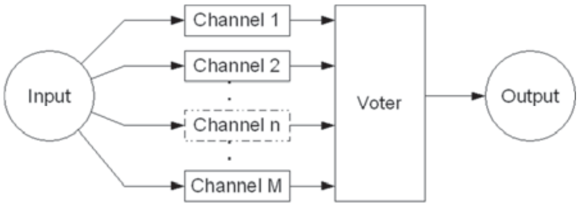

Fig. 1. The majority solution

Therefore by the authors of this article are examined devices with MTTF, which more or it is equal to the time of life of system.

This assumption is based on the state-of-art quality control of element base and technology of assembling devices reached the level, which ensures the necessary time of time to failure.

I.e., an increase in the reliability can ensure not only with fault resistance but by the perfection of devices – perfectness approach (1).

Moreover, many of the authors (1, 2) note that the use of the perfect devices entails absence of the maintenance (for example computer hardware).

2. Reliability function

Function of reliability of N elements:

$$\boldsymbol{R(t)} = \frac{\boldsymbol{n(t)}}{\boldsymbol{N}}, \tag{1}$$

where ***n(t)*** – failure free elements and N – number of all elements at the begin.

The failure rate:

$$\boldsymbol{\lambda(t)} = \frac{\boldsymbol{1}}{\boldsymbol{R(t)}} \cdot \left(\frac{\boldsymbol{-dR(t)}}{\boldsymbol{dt}}\right), \tag{2}$$

where $\frac{-dR(t)}{dt}$ is failure speed.

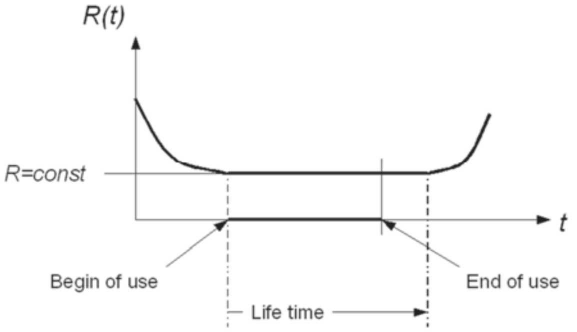

Fig. 2. Reliability function in time

The requirements of safety may be accept start of device use when $R = const$. The devices using from first moment is more economical beneficial for producer, but for end-user when evacuation (2.1) is feasible.

$$\frac{dR(t)}{dt} \to 0. \tag{2.1}$$

If evacuation (2.1) is not feasible then device is not ready for end-use.

3. Extended solutions

Is distinguished a certain number of checked solutions which make it possible to reach the specific level of failure tolerance or resistance. All these approaches have their advantages and disadvantages. Basis for these solutions again after all it is different levels assumption about the appearance of damage, failure in apparatus component or error in program component of system, subsystem or device. This makes it possible to make the conclusion that the purpose of construction is the safe or predictable functioning.

For example has introduced cold reserved solution for device with fault tolerance (fig. 3).

In the situation when device state controller notices fault or failure in main device the switching on reserve occurs (fig. 3.2) In some time if faulty or failure are caused by sudden faulty hazard source probability of damage for both devices exist.

Furthermore, the time of the hazard action is bigger at required switching time to reserve. The probability for both devices damage from one hazard source exists.

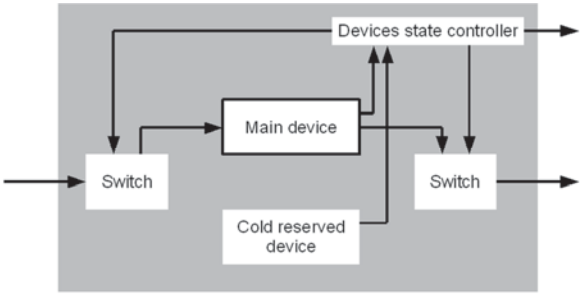

Fig. 3.1. Easy duplication

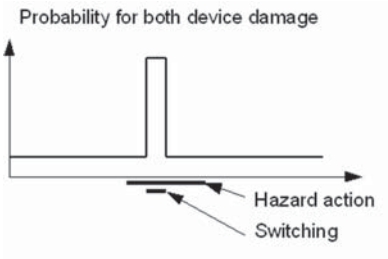

Fig. 3.2. The hazard action and switching time

4. Mega-system advantages

In present stage of the systems development, the subsystem or device are the parts of a mega-system (Fig. 4). Bulk of mega-system has a principle of construction – principle of cluster with localization or power distribution and has developed telecommunication. The expediency of constructing of the mega-system requires the independence of hierarchical higher located elements from lower located.

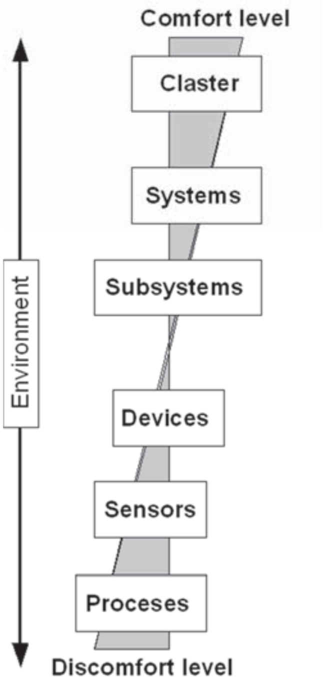

Fig. 4. Mega-system hierarchy

It should be noted that moving off from the cluster reduces the quality of operating conditions and as consequence an increase in the probability of the sudden failure.

An increase in the reliability must not be based only on the selection of the diagram of construction, but also must be dictated by decreasing in the vulnerability of the elements, which function at the uncomfortable level.

The followed article discuses this question. The value of the comfort for operating conditions is understood by many designers. Maintaining for conditions on the level of comfort is completely simple and efficient method, that guaranteeing the protection of devices, but also being expensive.

5. The probability of sudden failure

The statistical parameters of reliability, such as the function of reliability, the failure rate, MTTF sufficiently valid describe system, subsystem or device with the retention of the operating conditions of close ones to the conditions with which were obtained statistics, but in this case cause of failures or damage do not refine.

Testing for obtaining the statistics with the varied conditions for operation require the organization of the expensive and endurance of tests. I.e., most reliable are statistics those obtained at the appropriate level of comfort.

Let us examine the density of the distribution of the probability of the sudden failure, caused by operating conditions.

For this are used by annual or several annual cycles.

Probability of sudden failure POSF on the months:

$$\boldsymbol{P_i} = \frac{\sum_{M}^{Y=1} m_i(Y)\cdot AF_i(Y)}{\sum_{N}^{Y=1}\sum_{12}^{i=1} m_i(Y)}, \tag{3}$$

when $\boldsymbol{m_i(Y)}$ **–** number of failure in $\boldsymbol{i}$ – month in $\boldsymbol{Y}$ – year, caused by environment condition when object or objects observation in $\boldsymbol{M}$ of years, $\boldsymbol{AF_i(Y)}$ – availability factor in $\boldsymbol{i}$ – month in $\boldsymbol{Y}$ – year.

This statistics is valid, since observations were conducted the number of years.

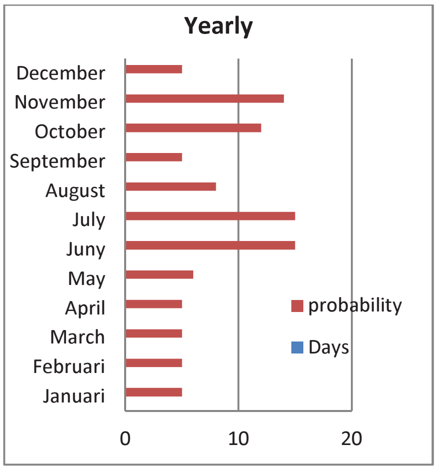

Fig. 5.1. Probability of sudden failure

For the devices of railway automatic is characteristic the presence of the closely spaced large metal constructions, electric power lines of high voltage, outlines of grounding, train rail.

From evacuation (3) follows that for decrease of POSF is necessary to exclude operation in the months of the greatest risk. Exception from the operation is not always possible. Then it is necessary the distance oneself from the source of hazard.

For the automatic systems they use several methods for distance of oneself from the most probable sources of hazard.

Most interesting and promising is the use of construction with the adapted availability factorAAF.

$$AF = {}^{MTBF}\!/_{(MTBF + MTTR)}, \tag{4}$$

when – $\boldsymbol{MTBF}$ – mean time between failures, $\boldsymbol{MTTR}$ – mean time to repair.

Adaptation is possible in the case, when exists separation toward the period of action and the waiting time.

$$\boldsymbol{MTBF = MTIO + MTIW,} \tag{5}$$

when $\boldsymbol{MTIO}$ – mean time in operation; $\boldsymbol{MTIW}$ – mean time in wait.

Adaptive availability factor:

$$AAF = {}^{MTIO}\!/_{(MTBF + MTTR)}. \tag{6}$$

I.e., this is completely permissible for the devices of railway automatic with specific traffic volume.

Adaptive construction provides for several required procedures:

1. Preparation for the exception from the system.
2. Estimation of availability for turning off.
3. Exception (complete or partial turning off) to the waiting time.
4. Estimation of readiness for the including.
5. Including.

Suppose $\boldsymbol{AF \approx 1}$ we will obtain:

$$AAF \approx {}^{MTIO}\!/_{MTIO + MWT} \tag{7}$$

Probability of sudden failure POSF on the months with adaptive availability factor:

$$\boldsymbol{P_i^{ADAPT}} = \frac{\sum_{M}^{Y=1} m_i(Y)\cdot AAF_i(Y)}{\sum_{N}^{Y=1}\sum_{12}^{i=1} m_i(Y)}, \tag{8}$$

When $\boldsymbol{AAF_i(Y)}$ – adaptive availability factor in $\boldsymbol{i}$-month in Y-year.

In (4) is the electronic gauge for diagnostic purpose via measurement introduced. For exception realization functional circuit needs local UPS (fig. 5.1).

The gauge is powered from local UPS in the wait mode operation that excepts device from hazard source such as high voltage power line.

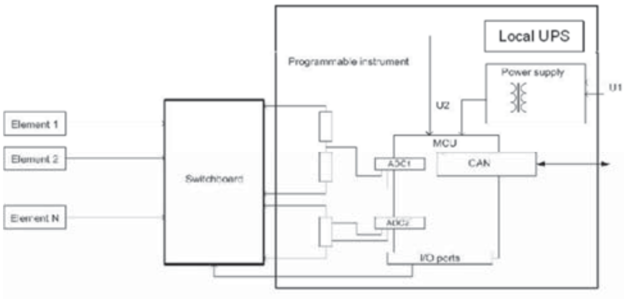

Fig. 5.1. Electronic gauge with local UPS

6. Achievement of failure tolerance with the presence of the upper level

Developed mega-system makes it possible to realize the principles of construction, not accessible or partially realized with the smaller possibilities.

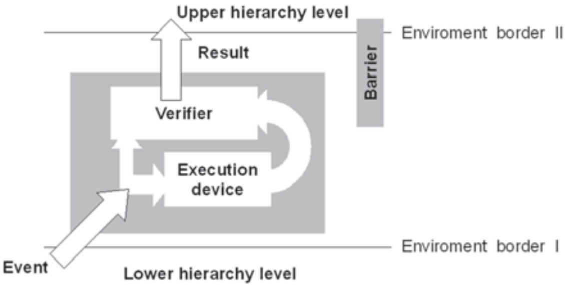

Fig. 6.1. Action I stage

Let us examine the construction of the element that consists of the executive device and verifier. It is complete construction with build testing equipment (BITE). Monitor changes its status by that verifier if it is ensured the exchange of information with the subsystem of upper level (fig. 6.1).

Thus event at the lower level causes in the execution device the reaction, which on the mean of verifier is evaluated and is transferred to the upper level.

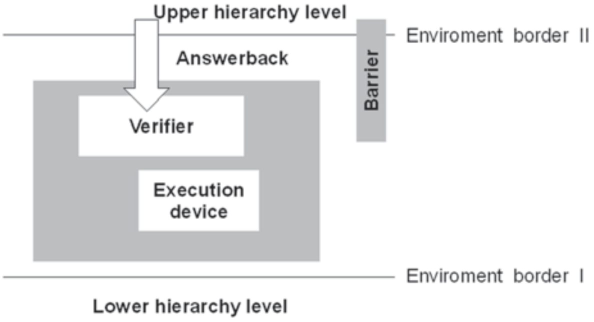

Fig. 6.2. Action II stage

Answerback contains information about both – the verifier and the execution device. In the following stage the verifier realizes quasi-event and is evaluated the reaction of execution device. In the case of the progress of verification the reaction to the event into the lower level is resolved (fig. 6.3 & fig. 6.4).

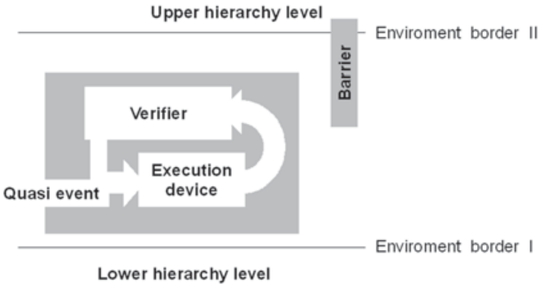

Fig. 6.3. Action III stage

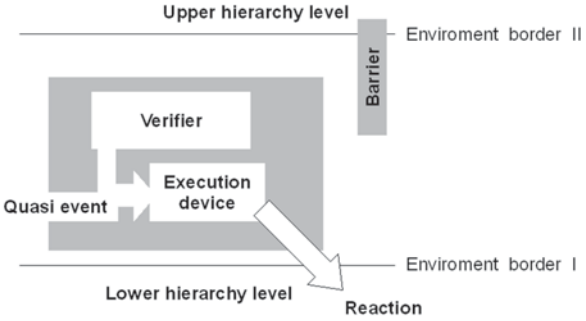

Fig. 6.4. Action III stage

This construction allowed:

1. To conduct the testing-verification before and after event, before and after the reaction on the event.
2. With the signs of the damage of execution device by the selection of quasi-event to cause the necessary reaction.
3. With the impossibility of quasi-event selection actuating element may be excluded from the action.
4. In the case of the uncontrollable functioning there is a possibility to use a barrier or "evacuation".

This construction can be the used and if the upper level is in the absence. Additional information about the state it is possible to obtain by using event – reaction memorizing (fig. 6.5).

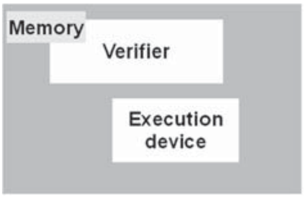

Fig. 6.5. Verifier with memory with upper level absence

Examined construction is based on contemporary of reaching in the telecommunication and computer technology, those accepted the basis level quality of services QoS in 0,999÷0,99999.

Conclusion

The statistical characteristics of reliability are the indices quality of performance for the object. In this case they do not contain answers to questions about the reasons of damages.

The requirement of failure tolerance or resistance dictates an increase in the protection of object, since the quality of performance leads to the absence of maintenance during the operation, but it does not protect from the sudden failure.

For end-user economical beneficial is devices with fault tolerance or resistance in comparison with requirements of comfort level guarding.

The exclusion or adaptive availability factor is way to decreasing for probability of sudden failure.

The presence of upper hierarchical level increases general protection in the case of the uncontrollable functioning of separate components.

Reference

Application of electronic gauges for automatic devices diagnostics. 2008. V. Karevs, M.Mezitis, 11-th Conference of Yong Scientists of Lithuania, “Science-Lithuania’s Future. *Transport*”.

Fault-Diagnosis System: An introduction from Fault Detection to Fault Tolerance. 2005. Isermann, Rolf.

Диагностика и надёжность автоматических систем. 2005. В. Н. Дианов, МГИУ.

Основы технической диагностики. 2004. В. В.Сапожников, Вл. В. Сапожников, Москва.