Failure Criteria and Time over Thresholds in Them

Victor Netes

•

Moscow Technical University of Communications and Informatics
v.a.netes@mtuci.ru

Abstract

A failure is one of the key concepts in dependability. Therefore, it is very important to distinguish whether a failure has occurred or not. To do this, a failure criterion is formulated. This article describes main approaches to determining failure criteria. Special attention is paid to the parametric approach, in which a failure is an event when one of the parameters characterizing the functioning of an item goes beyond the specified limits. In addition, a time over threshold can also be set. This means that short-term disruptions in item's operation are not considered as failures. The meaning of setting such a threshold is explained and examples of its use in telecommunications are given. For a parallel system with a time over threshold in a failure criterion, calculation formulas for dependability measures are derived. The errors that the use of traditional formulas gives in this situation are estimated.

Keywords: failure criterion, parametric approach, time over threshold, parallel system, MTBF, MTTR, availability

1. Introduction

The concept of a failure is one of the most important in the dependability theory. A failure of an item is defined as the loss of its ability to perform as required [1] (the terminology used in this paper mainly follows this basic international standard). In other words, a failure of an item is an event that transfers it from up to down state. Usually these two states are considered for an item in the reliability analysis: up or available state, in which it is able to perform as required, and down or unavailable state, in which it is unable to perform as required due to internal reason. Therefore, it is very important to distinguish between these two states.

As a rule, a failure criterion is introduced for this, which means a pre-defined condition for acceptance as conclusive evidence of failure [1]. The importance of the correct choice and formulation of failure criteria for reliability engineering is undeniable. In particular, one of the first popular books on reliability theory says [2, p. 14]: "We have placed great emphasis on the need for a clear-cut definition of the function of the device and its adequate performance on the one hand, and of failure or malfunction on the other".

In many works on reliability, it is assumed that the failure criterion has already been established in some way, but its exact formulation remains outside the scope of consideration. However, this can be done in various ways. Nevertheless, until now, insufficient attention has been paid to this issue, there is no sufficiently complete and clear description and analysis of possible approaches to determining a failure criterion in the literature. Perhaps the only field in which there are many publications devoted to this issue is materials science. It is easy to see by doing a Google search for the phrase "failure criterion". Even a special website is dedicated to this (https://www.failurecriteria.com).

This paper is devoted to eliminating this gap. It is organized as follows. Section 2 considers how a failure criterion can be determined. First, the two main approaches used for this are described. Then a time over threshold is introduced and explained. This means that short-term disruptions in item's operation are not considered as failures. The situations in which this may be appropriate are pointed out. The presence of such a threshold requires the correction of some well-known mathematical expressions and formulas used in reliability theory. They are discussed in the following sections. In section 3, the general mathematical model introduced in the classical monograph [3] is considered and its modification is proposed for the case of a time over threshold in the failure criterion. Section 4 explains why corrections in calculation formulas for dependability measures of a parallel system with time over threshold are required and the corrected formulas are derived. In this connection, the errors that the use of traditional formulas gives in this situation are estimated. At last, section 5 summarizes the main findings.

The presentation in section 2 is illustrated with specific examples from the field of telecommunications in which the author works. However, to understand them, the reader does not need to be an expert in this field; they will be understandable and useful to specialists in other industries. These examples are taken from the ITU-T documents. ITU-T is the Telecommunication Standardization Sector of the International Telecommunication Union (ITU). The International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and ITU form the World Standards Cooperation. ITU standards (called Recommendations) are fundamental to the operation of today's information and communication networks.

2. How a Failure Criterion Can Be Determined

2.1. Two Approaches to Determining a Failure Criterion

There are two approaches to the formulation of a failure criterion. They have been known for a long time and were mentioned in [2, p. 14]: "…In some simple cases, where devices of the "go–no go" type are involved, the distinguish between adequate performance and malfunction is a very simple matter. <…> But there are many more cases of a nature such that a clear-cut decision cannot be made so easily and a number of performance parameters and their limits must first be specified; operation within the limits is considered adequate or satisfactory, and outside of the specified limits it is considered inadequate".

Similar considerations are presented in the classical monograph [3, p. 71]. As a typical example of an item having a well-defined failure, an electric light bulb was given in it: "The operation of light bulb has, as a rule, two states: either it gives normal illumination or it gives no illumination at all". As an example of an item with a parametric failure assignment, a resistor was considered "for which the basic parameter determining quality is the magnitude of the resistance expressed in ohms".

Thus, these two approaches to determining the failure criterion can be called "go/no-go" and parametric. Similar two approaches exist when defining the general concept of "dependability" [4]. There is also an analogy here with two inspection methods in statistical quality control: inspection by attributes and inspection by variables [5].

It is worth mentioning that formally the go/no-go failure criterion can also be set parametrically. In this case, a binary parameter is used, which takes the value 1 in up state and the value 0 in down state. This is widely used, in particular, to describe the state of a system depending on the states of its elements by means of the structural function of the system [6]. In this case, the states of the elements and the entire system are characterized by binary variables (1 or 0).

In many cases, the failure criterion can be defined as a set of several conditions connected by a logical "or", i.e. the fulfillment of any of them is regarded as a failure. Some of these conditions may be "go/no-go", others may be parametric.

As the first example, consider analogue cable transmission systems and associated equipments. According to [7], a failure of such a system is considered to occur when there is:

1) complete loss of signal;

2) one in which the pilot level drops by 10 dB below nominal value;

3) when the total unweighted noise power, measured or calculated with an integrating time of 5 ms exceeds 1 million pW on the 2500 km hypothetical reference circuit.

The first condition has the go/no-go type. The second and third conditions are parametric. Each of them uses a specific parameter (the pilot level and the total unweighted noise power, the meaning of these parameters is not important for this consideration), for which a threshold value is set.

The Recommendation [7] is quite old. For more modern digital telecommunication networks, a parametric approach is used to determine a failure criterion. In general, it was formulated in [8]. Exactly, it says that the transitions between the available (up) and the unavailable (down) states based on events which are defined as occurring when the value of a function of a primary performance parameter(s) crosses a particular threshold.

2.2. A Time over Threshold in a Failure Criterion

When determining a failure criterion, a threshold value for time can also be used. As an example, consider again the failure criterion from [7]. In its above wording, the last phrase was omitted. However, it is very important. It reads: "In all instances, this condition must last at least 10 seconds". Thus, a time over threshold is introduced here. A similar situation takes place for other telecommunication systems. Often a threshold of 10 seconds is also used for them.

In general, there may be the following reasons to use a time over threshold:

- An item may have certain inertia, and a short-term disruption in its operation has no serious negative consequences.
- Using time over threshold allows reducing the number of alarms in fault management systems [9].
- The parameter used in the failure criterion may be statistical in nature, and obtaining a representative sample for its evaluation requires some time.

The latter situation is typical for modern telecommunications, where the main performance parameters used to formulate failure criteria are statistical in nature. For example, these are parameters such as the bit error rate, frame loss ratio, packet loss ratio, etc. In many cases, such a parameter is evaluated within a one second, the resulting value is compared with a certain threshold, in case of crossing which the second is regarded as "bad" (in each case, there is a special formal name for such a second). The failure criterion is the appearance of a certain number of "bad" seconds in a row.

As an example, consider technology Ethernet, which is widely used in computer networks. In such networks, data is transmitted in units called frames. A "bad" second occurs for a block of frames observed during a one-second interval when the corresponding frame loss ratio (i.e., the ratio of lost frames to total frames in the block) exceeds 0.5 [10].

Ten consecutive "bad" seconds are considered as a failure, i.e. the transition from the available state to the unavailable state. The corresponding 10-second period of time is considered to be part of unavailable time. The reverse transition from the unavailable state to the available state occurs when ten consecutive "not bad" seconds appear. The corresponding 10-second period of time is considered to be part of available time. All this is depicted in Fig. 1.

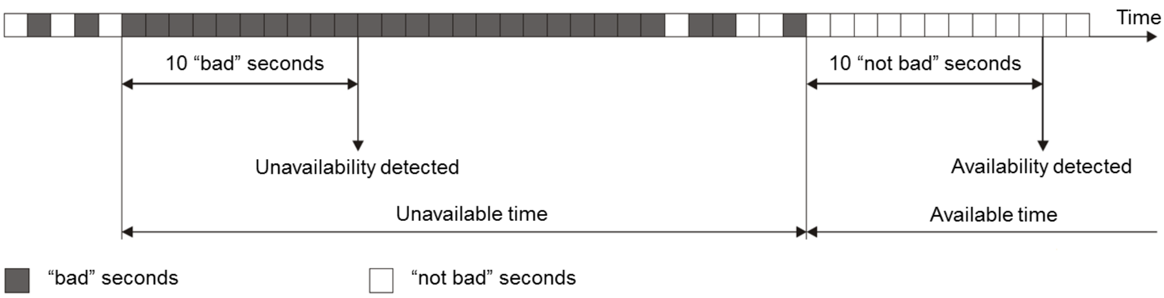

Figure 1: *Available and unavailable times with 10-second time over threshold*

3. A Time over Threshold in the General Set-Theoretic Model

In [3], a very general set-theoretic mathematical model was proposed to define and evaluate reliability measures. It is conceptual in nature and formed the basis for many further studies. It can be described as follows. Firstly, for the item under consideration, a set $S = \{x\}$ of states x is introduced that differ from each other in terms of reliability. It is called the phase space. For example, for the analogue cable transmission system discussed above, $x = (x_1, x_2, x_3)$, where x_1 is a binary variable that characterizes the presence ($x_1 = 1$) or loss ($x_1 = 0$) of the signal, x_2 is a non-negative variable equal to the pilot level, x_3 is a non-negative variable equal to the total unweighted noise power.

Then a random process with values in the phase space $x(t)$ is determined, which describes the change in the states of the item over time. Finally, the phase space S is divided into two disjoint subsets: S_1 and S_0 ($S_1 \cup S_0 = S$, $S_1 \cap S_0 = \emptyset$). If $x(t) \in S_1$, then at the moment t the item is in up state; if $x(t) \in S_0$, then at the moment t the item is in down state.

The moment of time $t^* > 0$ is the moment of failure, if and only if the following criterion is met:

$$(\exists \varepsilon > 0 \ \ \forall t \in (t^* - \varepsilon, t^*) \ \ x(t) \in S_1) \wedge (x(t^*) \in S_0). \tag{1}$$

The first condition in (1) means that immediately before the moment t^* an item was in up state, the second condition means that at the moment t^* it is in down state.

In this model, a reliability measure can be defined as the mathematical expectation of some functional $\Phi[x(t)]$ assigning numerical values to trajectories of the random process $x(t)$ [3]. For example, let

$$\Phi_1[x(t)] = \min \{ t^* > 0 \mid t^* \text{ satisfies (1)}\}. \tag{2}$$

Then, $\mathbf{E}\Phi_1[x(t)]$ is the mean operating time to the first failure ($\mathbf{E}$ is the symbol of mathematical expectation).

Another widely used measure is the reliability in the interval (t_1, t_2) (i.e., the probability of failure-free operation in this interval) $R(t_1, t_2)$. It is usually assumed that the item is in up state at the beginning of the time interval. $R(t_1, t_2) = \mathbf{E}\Phi_2[x(t)]$, where $\Phi_2[x(t)]$ is defined as

$$\Phi_2[x(t)] = \begin{cases} 1, \text{ if } \forall t \in (t_1, t_2) \ \ x(t) \in S_1; \\ 0, \text{ if } \exists t \in (t_1, t_2) \ \ x(t) \in S_0. \end{cases}$$

If there is a time over threshold in the failure criterion, the situation becomes more complicated. Indeed, the presence of the process $x(t)$ at the moment t at one or another point of the phase space no longer determines whether the item is currently in up or down state. This state depends on both the previous and future behavior of the process $x(t)$. The following are the appropriate formulations for this situation.

The phase space S is also divided into two disjoint subsets S_1 and S_0. However, in this case $x(t) \in S_1$ only means that at the moment t all the parameters used in the failure criterion are within the limits specified for them; $x(t) \in S_0$ means that at least one of these parameters has gone beyond these limits.

Denote the time over threshold by θ. Then the moment of time $t^* > \theta$ is the moment of failure, if and only if the following criterion is met:

$$(\ \exists t' < t^* - \theta\ \ (\forall t \in [t', t' + \theta]\ \ x(t) \in S_1)\ \wedge\ \overline{(\exists t'' \in [t' + \theta, t^*]\ \forall t \in [t'', t'' + \theta]\ x(t) \in S_0)}\ )\ \wedge$$
$$\wedge\ (\forall t \in [t^*, t^* + \theta]\ \ x(t) \in S_0). \quad (2)$$

The first and the second conditions in (2) together mean that immediately before the moment t^* an item was in up state (the overline means negation), the third condition means that starting from the moment t^* it is in down state.

The expectation of the functional $\Phi_1[x(t)]$, defined similarly to (2) with the replacement of (1) by (3), is equal to the mean operating time to the first failure. To determine $R(t_1, t_2)$, the functional $\Phi_2[x(t)]$ in this case takes the form

$$\Phi_2[x(t)] = \begin{cases} 1, \text{ if } \forall t' \in (t_1, t_2 - \theta)\ \exists t \in (t', t' + \theta)\ x(t) \in S_1; \\ 0, \text{ if } \exists t' \in (t_1, t_2 - \theta)\ \forall t \in (t', t' + \theta)\ x(t) \in S_0. \end{cases}$$

4. Calculation of Dependability Measures for a Parallel System with a Time over Threshold

The time over threshold also leads to the fact that adjustments have to be made to some well-known and widely used calculation formulas. In particular, this concerns formulas for mean operating time between failures (MTBF), mean time to restoration (MTTR) and availability of a parallel system.

Let the time over threshold θ be set for all elements and for the system as a whole. A parallel system is in down state if all its elements are in down state. However, periods of coincidence of down times of the elements can have different durations, both longer and shorter than θ. In the latter case, a system failure does not occur and such a short-term coincidence should not be considered as down time for the system. For the simplest example of a system having two parallel elements, this is shown in Fig. 2.

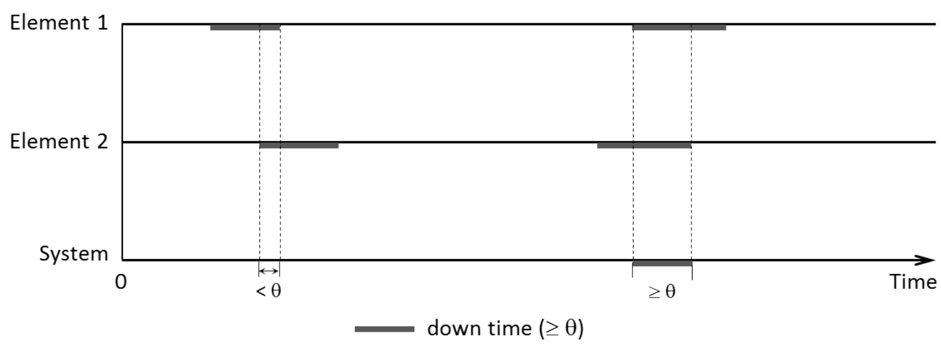

Figure 2: *Down time for a system of two parallel elements*

The traditional formulas do not take into account this circumstance. For most cases encountered in practice, the error in the calculation results will be very small. However, in order to evaluate it, it is necessary to be able to calculate dependability measures taking into account this circumstance, that is, to exclude short coincidences of downtime from consideration. The corresponding formulas will be derived below. To do this, a heuristic approximation is used, which gives good results for highly reliable systems [11, 12]. The higher the reliability, the more precise will be the result.

Consider a system of two independent parallel elements (as in Fig. 2). Let T_i and τ_i denote, respectively, the MTBF and the MTTR of the ith element, $i = 1, 2$. They are determined taking into account the time over threshold θ in the failure criteria. To apply the heuristic approximation, it is assumed that $T_i >> \tau_i$. In practice, this condition is usually met. The distribution function for the time to restoration of the ith element is denoted by $G_i(t)$. When $t \le \theta$, $G_i(t) = 0$.

Denote by T_0 and τ_0 the MTBF and the MTTR of the system, calculated without taking into account the time over threshold, and the same measures determined taking the threshold into account are denoted by T and τ. For T_0 and τ_0 there are the following formulas [11]:

$$T_0 \approx \frac{T_1 T_2}{\tau_1 + \tau_2}, \tag{3}$$

$$\tau_0 \approx \frac{\tau_1 \tau_2}{\tau_1 + \tau_2}. \tag{4}$$

The duration of a coincidence of elements' down times is the residual restoration time of the element that failed first, starting from the moment of failure of another element. This residual restoration time of the ith element has the density function $[1 - G_i(t)]/\tau_i$ [13]. Therefore, the probability q_i that this time for the ith element is less than θ can be calculated as follows:

$$q_i = \int_0^\theta \frac{1 - G_i(t)}{\tau_i} dt = \frac{\theta}{\tau_i}.$$

The total flow of coincidences has the rate $\lambda_0 \approx (\tau_1 + \tau_2)/(T_1 T_2)$ [9]. The coincidences in which the ith element fails first form a flow with the rate $\lambda_{0i} \approx \tau_i/(T_1 T_2)$. So, the probability that the ith element initially fails when a coincidence occurs, $\pi_i = \lambda_{0i}/\lambda_0 \approx \tau_i/(\tau_1 + \tau_2)$. Hence, for the probability that the duration of a coincidence is less than θ, we get:

$$q = \pi_1 q_1 + \pi_2 q_2 = \frac{\tau_1}{\tau_1 + \tau_2} \cdot \frac{\theta}{\tau_1} + \frac{\tau_2}{\tau_1 + \tau_2} \cdot \frac{\theta}{\tau_2} = \frac{2\theta}{\tau_1 + \tau_2} . \tag{5}$$

Using (3) and (5), the MTBF of the system can be calculated as follows:

$$T = \frac{T_0}{1 - q} \approx \frac{T_1 T_2}{\tau_1 + \tau_2} \cdot \frac{\tau_1 + \tau_2}{\tau_1 + \tau_2 - 2\theta} = \frac{T_1 T_2}{\tau_1 + \tau_2 - 2\theta} . \tag{6}$$

To compare T and T_0, their ratio is calculated. It follows from (3) and (6) that

$$\frac{T}{T_0} \approx \frac{\tau_1 + \tau_2}{\tau_1 + \tau_2 - 2\theta} . \tag{7}$$

Hence when $\theta << \tau_i$

$$\frac{T}{T_0} \approx 1 + \frac{2\theta}{\tau_1 + \tau_2}\ . \tag{8}$$

The mean duration of a short (less than θ) coincidence is θ/2. Therefore, the following equality holds:

$$\tau_0 = q(\theta/2) + (1 - q)\tau. \tag{9}$$

Expressing τ from (9) and substituting τ_0 from (4) and q from (5), we get:

$$\tau \approx \frac{\tau_1\tau_2 - \theta^2}{\tau_1 + \tau_2 - 2\theta}\ . \tag{10}$$

From (4) and (10), under the same condition $\theta \ll \tau_i$, an expression similar to (8) can be obtained:

$$\frac{\tau}{\tau_0} \approx 1 + \frac{2\theta}{\tau_1 + \tau_2}.$$

For example, if $\tau_i/\theta \approx 100$, not taking into account the time over threshold when calculating the MTBF and the MTTR of the system gives a relative error of about 1 %. However, if $\tau_i/\theta \approx 5$, the error will be about 20…25 %.

Availability and unavailability of the system can be calculated based on its MTBF and MTTR. In this case, it is advisable to compare the unavailability, which using (6) and (10) is expressed as

$$U = \frac{\tau}{T + \tau} \approx \frac{\tau_1\tau_2 - \theta^2}{T_1T_2 + \tau_1\tau_2 - \theta^2}\ . \tag{11}$$

Since $\theta < \tau_i \ll T_i$, it follows from (11) that

$$U \approx \frac{\tau_1\tau_2 - \theta^2}{T_1T_2} = \frac{\tau_1\tau_2}{T_1T_2} - \frac{\theta^2}{T_1T_2}.$$

In the traditional calculation, $U_0 = U_1U_2$, where $U_i = \tau_i/(T_i + \tau_i)$ is the unavailability the ith element. When $\tau_i \ll T_i$, $U_i \approx \tau_i/T_i$. Therefore $U_0 \approx (\tau_1\tau_2)/(T_1T_2)$, from which it follows that

$$U \approx U_0 - \frac{\theta^2}{T_1T_2}\ . \tag{12}$$

It can be seen from (12) that the difference between the values of unavailability U and U_0 is significantly less than for MTBF and MTTR. This is quite natural, since, as was shown above, the relative errors from not taking into account the time over threshold when calculating MTBF and MTTR are approximately the same, and the unavailability depends only on the ratio MTBF/MTTR.

Similar formulas can be derived for parallel systems with a number of elements greater than two, although rather cumbersome expressions are obtained. For example, for a system of three elements, they have the form:

$$T \approx \frac{T_1T_2T_2}{\tau_1\tau_2 + \tau_1\tau_3 + \tau_2\tau_3 - 2\theta(\tau_1 + \tau_2 + \tau_3) + 3\theta^2},$$

$$\tau \approx \frac{\tau_1\tau_2\tau_3 - \theta^2(\tau_1 + \tau_2 + \tau_3) + 2\theta^3}{\tau_1\tau_2 + \tau_1\tau_3 + \tau_2\tau_3 - 2\theta(\tau_1 + \tau_2 + \tau_3) + 3\theta^2},$$

$$U \approx \frac{\tau_1\tau_2\tau_3 - \theta^2(\tau_1 + \tau_2 + \tau_3) + 2\theta^3}{T_1 T_2 T_2}.$$

These formulas were obtained as follows. Initially, the first and second elements were replaced by one element, MTBF and MTTR for which were taken in accordance with (6) and (10), respectively. This element was then combined with the third element.

5. Conclusion

The main findings of this article are as follows.

- When specifying quantitative dependability requirements for an item, a failure criterion should be formulated for it. In particular, this can be done in a parametric way. This means that some performance parameters are selected and acceptable limits are set for them. When one of the parameters drifts out of its limits, a failure is fixed.
- A time over threshold can also be set in a failure criterion. This means that short-term disruptions in item's operation lasting less than this threshold are not considered as failures.
- The presence of a time over threshold requires correction in calculation formulas for dependability measures of parallel systems. However, when this threshold is much less than the mean times to restoration of elements, the error from applying traditional formulas will be insignificant.

References

[1] IEC 60050-192:2015. International Electrotechnical Vocabulary – Part 192: Dependability.

[2] Bazovsky, I. Reliability: Theory and Practice, Prentice-Hall, 1961.

[3] Gnedenko, B. V., Belyayev, Yu. K., Solovyev, A. D. Mathematical Methods in Reliability Theory, Academic Press, 1969.

[4] Netes, V. A., Tarasyev, J. I., Shper, V. L. (2014). How we should define what "dependability" is. *Dependability*, 4: 15–26.

[5] ISO 3534-2:2006. Statistics – Vocabulary and symbols – Part 2: Applied statistics.

[6] Barlow, R. E., Proschan, F. Mathematical Theory of Reliability, John Wiley & Sons, 1965.

[7] ITU-T Recommendation G.602 (1984). Reliability and Availability of Analogue Cable Transmission Systems and Associated Equipments.

[8] ITU-T Recommendation I.350 (1993). General Aspects of Quality of Service and Network Performance in Digital Networks, Including ISDNs.

[9] Sylor, M. and Meng, L. (2000). Using time over threshold to reduce noise in performance and fault management systems. *Lecture Notes in Computer Science*, 1960: 145–156.

[10] ITU-T Recommendation Y.1563 (2009). Ethernet Frame Transfer and Availability Performance.

[11] Kozlov, B., Ushakov, I. Reliability Handbook, Holt, Rinehart and Winston, 1970.

[12] Handbook of Reliability Engineering, ed. Ushakov, I. A. John Wiley & Sons, 1994.

[13] Feller, W. An Introduction to Probability Theory and Its Applications, John Wiley & Sons, New York, 1971, vol. 2.