Annals of Nuclear Energy 87 (2016) 537–540

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Impact of proof test interval and coverage on probability of failure of safety instrumented function

Jianghong Jin [a,b,*], Lei Pang [c], Bin Hu [a], Xiaodong Wang [a]

[a] Beijing Municipal Institute of Labor Protection, PR China
[b] China Academy of Safety Science and Technology, PR China
[c] Beijing Institute of Petrochemical Technology, PR China

ARTICLE INFO

Article history:
Received 17 February 2014
Received in revised form 28 September 2015
Accepted 29 September 2015
Available online 20 October 2015

Keywords:
Safety instrumented system
Imperfect proof test
Average probability of failure on demand
Probability of test independent failures (P_{TIF})
Reliability block diagram (RBD)

ABSTRACT

Imperfection of proof test can result in the safety function failure of safety instrumented system (SIS) at any time in its life period. IEC61508 and other references ignored or only elementarily analyzed the imperfection of proof test. In order to further study the impact of the imperfection of proof test on the probability of failure for safety instrumented function (SIF), the necessity of proof test and influence of its imperfection on system performance was first analyzed theoretically. The probability of failure for safety instrumented function resulted from the imperfection of proof test was defined as probability of test independent failures (P_{TIF}), and P_{TIF} was separately calculated by introducing proof test coverage and adopting reliability block diagram, with reference to the simplified calculation formula of average probability of failure on demand (PFD_{avg}). Research results show that: the shorter proof test period and the higher proof test coverage indicate the smaller probability of failure for safety instrumented function. The probability of failure for safety instrumented function which is calculated by introducing proof test coverage will be more accurate.

1. Introduction

In order to verify the operation status of safety instrumented system and confirm its safety integrity level (SIL), periodic proof test of safety instrumented system must be conducted. The proof test is also called periodic test (IEC61511-1, 2003; IEC61508-4, 2010), and refers to test of the whole system, including sensor, logic controller, final executive mechanism and some relevant alarms. However, not all failures of the safety instrumented system can be completely detected through self-diagnostic test. Proof test just aims to find the failures of the safety instrumented system undetected through self-diagnostic test, so as to reduce the rate of failures undetected by a single device. But the actual proof test is non-ideal and imperfect, and the failure undetected through self-diagnostic test can be detected only in some probability, and cannot be completely detected. The failures undetected by proof test will be passed on and accumulated to next proof test, until they are found when process has a safety function demand, i.e. safety instrumented system sooner or later will encounter safety instrumented function failures caused by the dangerous failures undetected by proof test, which will cause accidents. Therefore, it is necessary to deeply study the influence of the imperfect proof test on the probability of failure for safety instrumented function. There are many researches on the time interval rationality of test for each subsystem or device of safety instrumented system (Adamski, 2002; Sungwhan and Jin, 2008; EXIDA, 2013). Urbanik (2004) studied the reliability of release valve during the period of test and maintenance. Lundteigen and Rausand (2007) implement defense measures through function testing to reduce common cause failures in safety instrumented systems on oil and gas installations. They all did not study the imperfection of proof test, however. The old version of IEC61508-6 (2000) did not consider the imperfection of proof test, which is equivalent to that the assumed proof test coverage is 100%, which obviously is not reasonable. The new version of IEC61508-6 (2010) pointed out that justification should be given for the assumptions of restoration to "as good as new" after proof test, but it still did not quantify the influence of imperfect test on the probability of failure for safety instrumented function. Goble (1998), Goble and Cheddie (2006), and Bai et al. (2008) pointed out that, when verifying the PFD_{avg} in low demand mode of operation, people should consider the proof test coverage factor, and give a method of PFD_{avg} for single channel. Yang and Guo (2007) and Guo (2009) mentioned the efficiency of testing, and simply discussed its effect on the probability of failure for

* Corresponding author at: No. 55 Taoranting Road, Beijing 100054, PR China. Tel.: +86 10 63524189x201; fax: +86 10 83559840.
E-mail address: kathy_jinjh@126.com (J. Jin).

http://dx.doi.org/10.1016/j.anucene.2015.09.028
0306-4549/

safety function. Hauge et al. (2006a) described the system failures undetected by the proof test with test independent failures (TIF), and its probability of failure for safety instrumented function is denoted by P_{TIF} which is directly presented by the database of standard industry method (Hauge et al., 2006b). In summary, there is no systematic and deep research on the imperfection of proof test and its probability of failure for safety instrumented function. This paper puts forward the concept of proof test coverage to describe the imperfection of proof test, and deeply analyzes the influence and contribution of the proof test coverage to the probability of failure for safety instrumented function.

2. Necessity and imperfection influence of proof test

People can better understand the necessity of proof test from the formula of the PFD_{avg}. For example, when the pressure protection safety instrumented system with a simple 1oo1 (1 out of 1) voting architecture executes the demand of pressure protection function; the PFD_{avg} of pressure transmitter is shown as Eq. (1).

$$PFD_{avg} = \lambda_{DU} \cdot \frac{\tau}{2} \tag{1}$$

where, λ_{DU} is the dangerous undetected failure rate, and τ is the period of proof test. Seen from Eq. (1), PFD_{avg} is proportional to proof test period and the dangerous failure rate (λ_{DU}) of the device, (for example, not opening on demand), i.e. the proof test period and the dangerous failure rate of the device are also very important to PFD_{avg}. In theory, if safety instrumented system is not subject to proof test, then $\tau = 0$ and $PFD_{avg} = 0$, in other words, the system cannot normally respond when necessary. Therefore, the proof test is very necessary.

Proof test can be automatic or manual, and is specific to both hardware and software. Just as mentioned above, proof test just aims to find the failures undetected through self-diagnostic test, especially the dangerous failures. But because of unknown failure mode, technical level of proof test and the quality of test personnel, proof test will be imperfect. Potential dangerous failures can be found only in some probability, and this paper defines this probability as the proof test coverage. The range of proof test coverage is related to many factors, especially the human factors. If the assumed test period is τ, and proof test coverage is c_τ, the rate of failures undetected by proof test will be passed on and accumulated to next proof test in $(1 - c_\tau)\ \lambda_{DU}$, until it is found when the process has the demands of safety function. That is to say, the failure undetected by proof test possibly will always exist in the system life period, thus causing the increase of the probability of failure for safety instrumented function. For example, if partial stroke test is used to replace the whole stroke test in the process of valve testing, the valve will increase the possibility of failures because it has not completely passed the test verification.

In addition, what should be pointed out is that, different failures undetected will have different proof test coverage, but they are not distinguished in this paper and are all marked as c_τ.

3. Analysis on the probability of failure for safety instrumented function based on different dangerous failure rates

After comprehensive consideration of self-diagnostic test and proof test, the dangerous failure rate of a single device consists of three parts, as shown in Fig. 1. λ_{DD} detected through self-diagnostic test (including personnel's routing inspection); λ_{DU1} detected by proof test rather than self-diagnostic; λ_{DU2} that cannot be detected by proof test and but can be found only when the process has the demand of safety function. In consideration of the proof test coverage c_τ, λ_{DU1} (that can be detected by periodic test) = $c_\tau\ \lambda_{DU}$, and λ_{DU2} (that cannot be detected by periodic test) = $(1 - c_\tau)\ \lambda_{DU}$. All dangerous failure rates are respectively used for the performance evaluation calculation model of safety instrumented system. Here we will only pay close attention to PFD_{avg} related to proof test (the average probability of failure on demand for safety instrumented system caused by λ_{DU1} and λ_{DU2} are temporarily defined as PFD_{avg}), instead of discussing the probability of failure for safety instrumented function which is caused by λ_{DD}.

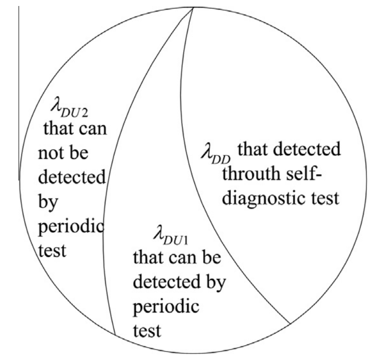

Fig. 1. Illustration of composition of single device dangerous failure rate λ_D.

Eq. (1) assumes proof test coverage as 1, which is ideal. But in fact, it is very difficult to find out all potential dangerous failures by proof test, and some dangerous failures still exist in the whole life period of the system instead of being found. At this moment, PFD_{avg} should consist of the probability of failure for safety instrumented function caused by two kinds of dangerous failures (λ_{DU1} and λ_{DU2}). Therefore, the more accurate expression of PFD_{avg} is shown in Eq. (2).

$$PFD_{avg} = c_\tau \cdot \lambda_{DU} \cdot \frac{\tau}{2} + (1 - c_\tau)\lambda_{DU} \cdot \frac{SL}{2} \tag{2}$$

where, SL is system life.

To further understand the impact of proof test, this paper carries out the discussions as follows:

The dangerous failure rate of close valve is 0.025 times/year, and the proof test coverage is set as 95%. If no proof test of this valve is conducted, this valve will be replaced by a new one after working for 10 years. According to Eq. (1), the PFD_{avg} is:

$$PFD_{avg} = \lambda_{DU} \cdot \frac{\tau}{2} = 0.025 \times \frac{10}{2} = 0.125$$

If the proof test of this valve is conducted one time each year, it will be replaced by a new device after working for 10 years. According to Eqs. (1) and (2), the PFD_{avg} is respectively:

$$PFD_{avg} = \lambda_{DU} \cdot \frac{\tau}{2} = 0.025 \times \frac{1}{2} = 0.0125$$

$$PFD_{avg} = c_\tau \cdot \lambda_{DU} \cdot \frac{\tau}{2} + (1 - c_\tau)\lambda_{DU} \cdot \frac{SL}{2}$$
$$= 0.95 \times 0.025 \times \frac{1}{2} + (1 - 0.95) \times 0.025 \times \frac{10}{2} = 0.018$$

According to the example calculation results (0.125 and 0.0125), proof test conducted one time each year will reduce the PFD_{avg} of safety instrumented system with the 10-years lifetime by 10 times. It is thus clear that, the proof test is essential for ensuring the performance of safety instrumented system.

According to example calculation results (0.0125 and 0.018), the PFD_{avg} without consideration of proof test coverage calculation is a little bit lower, and the actual PFD_{avg} of safety instrumented system is higher, so it actually masks the potential risk of safety instrumented system, and increases the accident risk in the