Mean fault time for estimation of average probability of failure on demand PFD_{avg}.

Isshi KOYATA[a]*, Koichi SUYAMA[b], and Yoshinobu SATO[c]

[a] The University of Marine Science and Technology Doctoral Course, Course of Applied Marine Environmental Studies , Tokyo, Japan
Japan Automobile Research Institute, Tokyo, Japan

[b] The University of Marine Science and Technology Doctoral Course, Professor, Tokyo, Japan

[c] Japan Audit and Certification Organization for Environment and Quality, Tokyo, Japan

Abstract: In functional safety standards, the safety integrity of safety-related system operated in the low demand-mode of operation is defined as its average probability of dangerous failure on demand, PFD_{avg}. In this paper, we firstly formulate the PFD_{avg} resulting from the undetected failures being maintained by proof tests from the two-viewpoints of the mean fault time, the reliability, and the risk assessment of safety-related system. Based on the formulation, the mean fault time is derived using the proof test interval for 1-out-of-n redundant systems. The mean fault time is useful for the exact estimation of safety integrity using Markov-state transition diagrams.

Keywords: Functional safety standard, Safety integrity, Low demand mode of operation, PFD_{avg}

1. INTRODUCTION

Basic safety standard IEC61508 that defined the Functional safety of electrical/electronic/ programmable electronic safety-related system (as below safety-related system) is classified as a low demand mode and continuous or high demand mode of the safety-related system operation mode.
In standard safety integrity level at a low demand mode derived that the average probability of dangerous failure on demand, i.e., PFD_{avg} multiplied by demand rate.

PFD_{avg} is derived from using mean fault time between proof test intervals of safety-related system.

This paper introduces the average probability of dangerous failure on demand, i.e., PFD_{avg} by two view points of reliability and hazardous or harmful event rate.
And so on, from the results of two viewpoints it provide the method of introduce the mean fault time at redundant system.

2. HAZARDOUS OR HARMFUL EVENT LOGIC

There are two states of hazardous or harmful event logic, namely:

- Event logic 1 in case of that safety related system is failure state at at first and then demand occurs; and

- Event logic 2 in case of that safety-related system is demand state at first and then failure occurs.

The relationship of two states of hazardous or harmful event logic is depicted in Figure 1.

---

* ikoyata@jari.or.jp

Event logic 1 is equivalent to low demand mode of safety related system, and event logic 2 is equivalent to high demand or continuous mode of safety related system.

In this paper the mean fault time is derived from the results of formulated PFD_{avg} at three case view points for derive the mean down time between proof tests in low demand mode.

It is recommended that safety integrity level, i.e., failure (risk) event rate is evaluated correctly not only to use PFD_{avg} but also to use the Markov graph modeling.

It is mandatory to use the mean down time at modeling of the repair about the Dangerous Undetected failure.

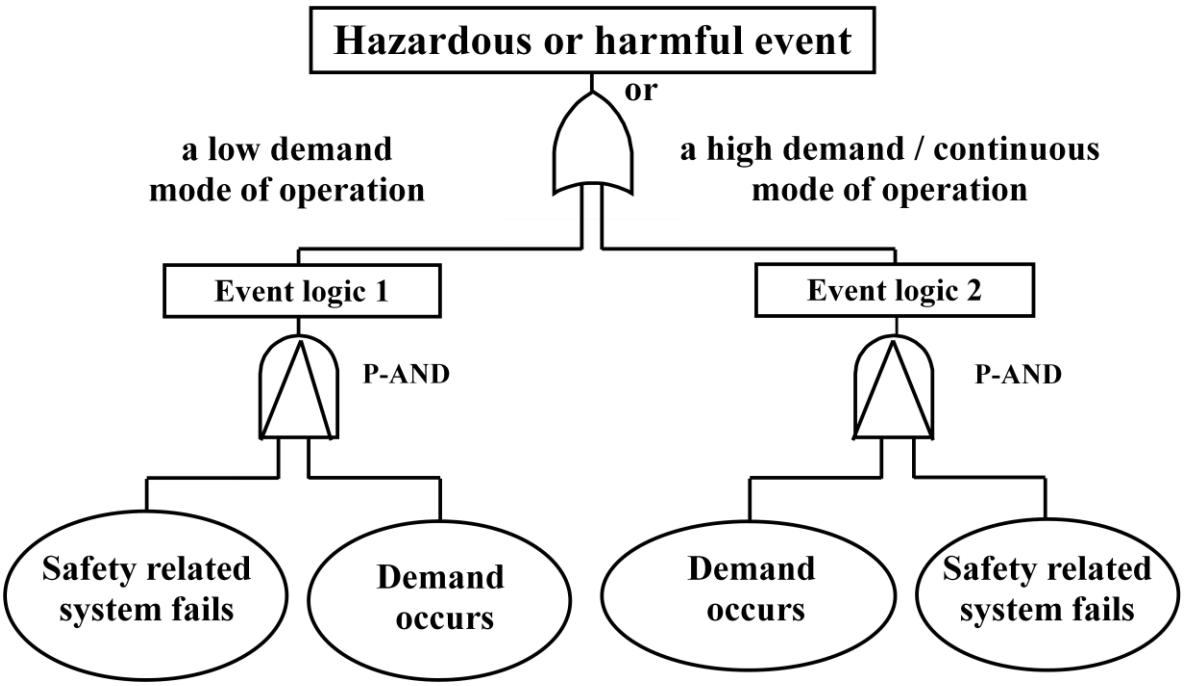

Figure 1 - The concept of hazardous or harmful event

3. BASIC FORMULATION

3.1. Average probability of dangerous failure on demand; PFD_{avg}

PFD_{avg} is expressed as "average probability of dangerous failure on demand" in Part-4 : "Definitions & abbreviations" of Functional safety standards IEC61508.
In standard NOTE 2; PFD_{avg} is expressed as "the dangerous undetected failures occurred since the last proof test and genuine on demand failures caused by the demands (proof tests and safety demands) themselves".

In functional safety standard; IEC61508 Part-1: General requirements, IEC61508 requires that safety integrity level is introduced from "the average probability of dangerous failure on demand of functional safety".

The dangerous failures on demand of safety function are occurred by dangerous detected failure by self test and dangerous undetected failure by repair at proof test not by self test.

In this report, later, it is focused on only dangerous undetected failure.
And the time of proof test and repair time are ignored small enough compared to the time interval of proof test : T.

The relationship between proof test and item status is shown in Figure 2.

Where
T is the time interval of proof test;
K (n) is the number of the proof test time meaning of K(1, 2, 3, ... , n, n+1) ;

T_a is the normal state time from restoration occurs at (K+1)-th proof test to failure for the 1-st time occurs during (n, n+1] proof test; and
T_b is the fault time from failure to restoration occurs during (n, n+1]-th proof test.

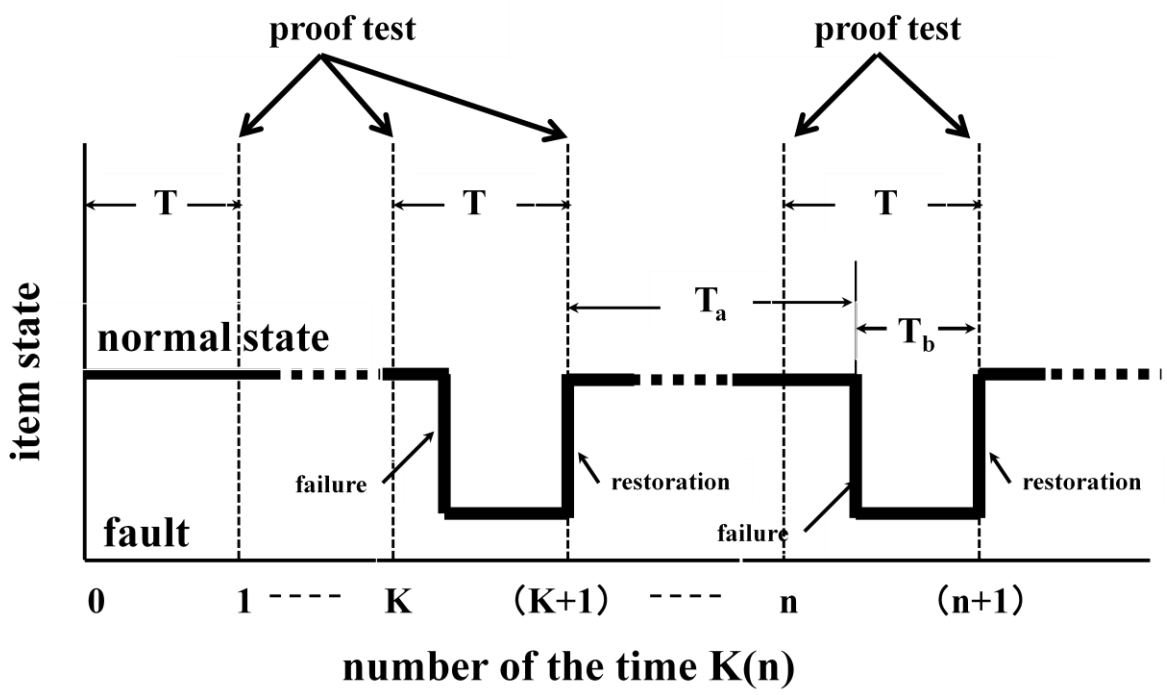

Figure 2 - Relationship between proof test and status of item

PFD_{avg} is derived by the following formula from the relationship T_a*+T_b*.

$$PFD_{avg} = T_b^* / (T_a^* + T_b^*) \quad (1)$$

Where
T_a* is the mean time of T_a; and
T_b* is the mean time of T_b.

T_a* and T_b* are derived by mean of T_a and T_b as below;

$$T_a^* = \frac{1}{l}\sum_{i=1}^{l} T_a\ i \quad (2)$$

$$T_b^* = \frac{1}{m}\sum_{j=1}^{m} T_b\ j \quad (3)$$

Further T_a* is derived by failure rate of dangerous undetected failure.

$$T_a^* = 1 / \lambda_{DU} \quad (4)$$

PFD_{avg} is derived by the following formula from Figure 2 and the above relationship.

$$PFD_{avg} = T_b^* / (T_a^* + T_b^*) = T_b^* / (1/\lambda_{DU} + T_b^*) \fallingdotseq T_b^* \lambda_{DU} \quad (5)$$

(because $1 / \lambda_{DU} \gg T_b^*$)

As above, "average probability of dangerous failure on demand", i.e. , PFD_{avg} is described by the relationship of up state and down state of item in proof test.

3.2. Failure distribution function of 1-out-of-1 system

Failure distribution function of each system is described in order to derive the PFD_{avg} in each viewpoints.

Failure distribution function of series system, i.e., 1-out-of-1 system is described.

Failure distribution function is set to F (t) and F (t) is sufficiently smaller than 1.

$$F(t) \cong \lambda_{DU} t \ll 1 \quad (6)$$

From a series system of 1-out-of-1, the failure distribution function in proof test interval is mentioned to Figure 3.

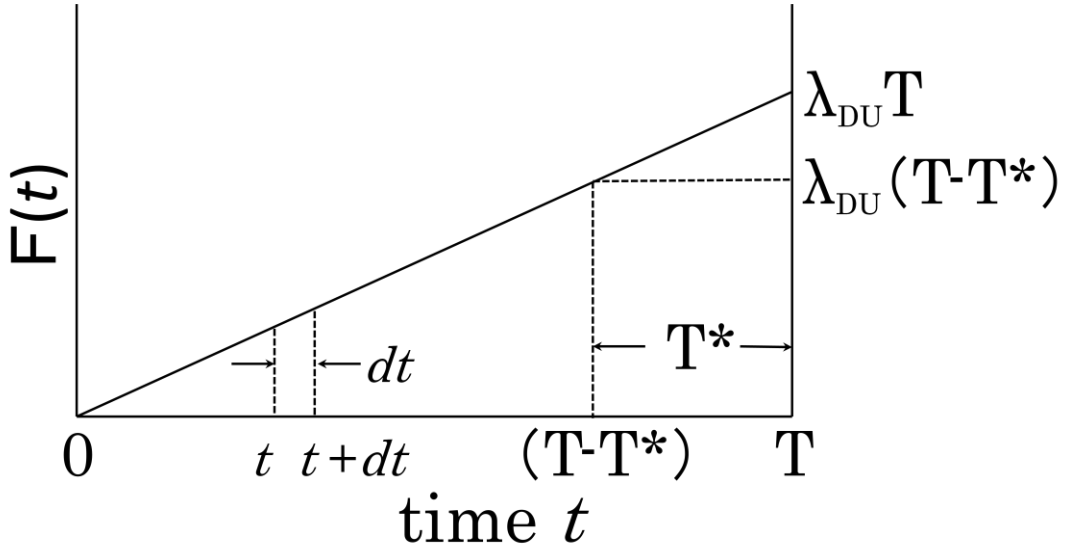

Figure 3 - a failure distribution function of 1-out-of-1 system

Figure 3 shows a failure distribution function of 1-out-of-1 system

Where
T is proof test interval; and
T* is the mean fault time.

3.3. Failure distribution function of 1-out-of-n system

It is derived from the relationship in 1-out-of-n system of redundant system.

When I set the failure distribution function (unreliability) equal F (t), from a redundant system,

$$F(t) \cong \lambda_{DU} t \ll 1 \qquad (7)$$

From a redundant system of 1-out-of-n, the failure distribution function in proof test interval is mentioned to Figure 4.

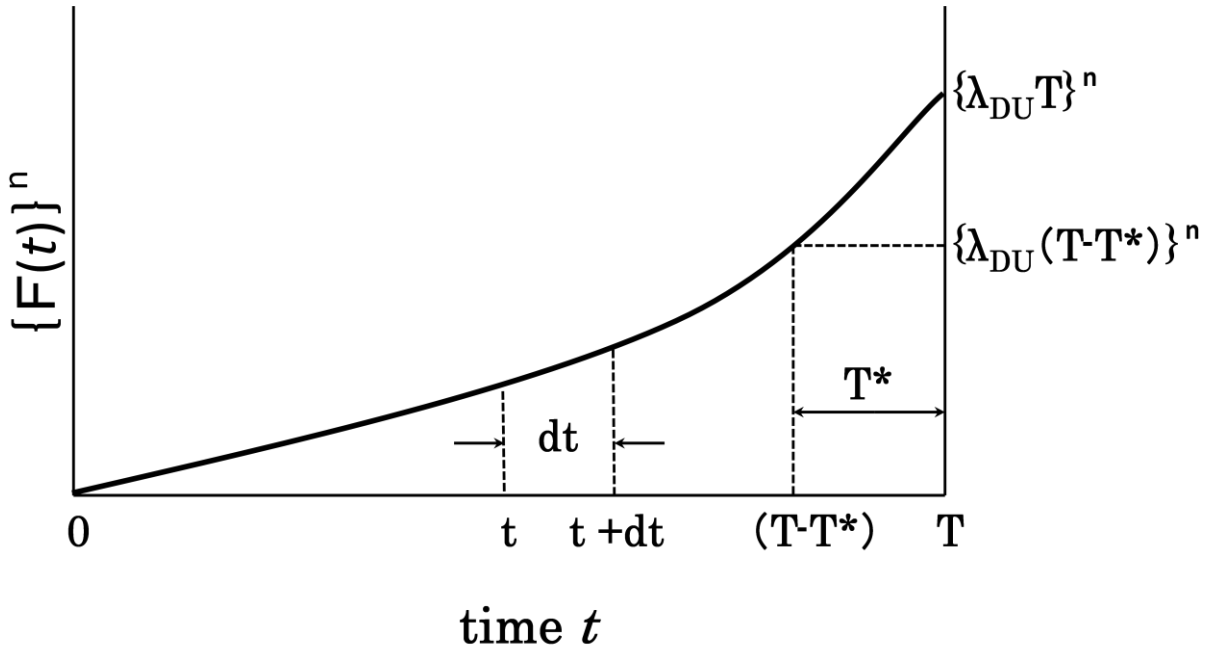

Figure 4 - a failure distribution function of 1-out-of-n system

Figure 4 shows a failure distribution function of 1-out-of-n system

Where
T is proof test interval; and
T* is the mean fault time.

3.4. Relationship between mean fault time and PFD_{avg}

It is derived from mean fault time of 1-out-of-n system to PFD_{avg}.

This means that the system fails at proof test interval during (0, T], and demand occurs at from during ((T-T_b*) to T].

In this condition PFD_{avg} is

PFD_{avg} = Pr {system fails at proof test during (0, T), and system fails from during (T-T_b*) to T at demand occurs during (0, T]. (8)

That is

PFD_{avg} = Pr {system fails at proof test during (0, T)} Pr{demand occurs during (T- T_b*, T] | demand occurs during (0, T]}

= Pr {system fails at proof test during (0, T)} Pr {demand occurs during (T- T_b*, T] / Pr {demand occurs during (0, T] }

= Pr {system fails at proof test during (0, T)} (T_b^* / T)

= $\{F(T)\}^n(T_b^* / T)$

= $\{\lambda_{DU}T\}^n(T_b^* / T)$ (9)

In condition of Figure 4, average probability of functional failure on demand is

$PFD_{avg} = \{\lambda_{DU}T\}^n (T_b^* / T)$ (10)

4. TWO METHODS FOR DERIVATION OF PFD_{avg}

4.1. Calculation of reliability

It is derived from reliability of 1-out-of-n system to PFD_{avg}.

PFD_{avg}=

$$\int_0^T \Pr\{\text{system fails during } (t, T+dt] \text{ , and demand occurs during } (t, T] \text{ in proof test }\}dt \quad (11)$$

That is

PFD_{avg} =

$$\int_0^T \Pr\{\text{system fails during } (t, T+dt] \text{ , and demand occurs during } (t, T] \text{ in proof test }\}dt$$

$$= \int_O^T nF(t)^{n-1}\frac{(T-t)}{T}\lambda_{DU}dt$$

$$= \int_O^T n\{\lambda_{DU}t\}^{n-1}\frac{(T-t)}{T}\lambda_{DU}dt$$

$$= \int_O^T n\{\lambda_{DU}t\}^{n-1}\frac{(T-t)}{T}\lambda_{DU}dt$$

$$= n\lambda_{DU}^n\int_O^T t^{n-1}dt - n\lambda_{DU}^n\frac{1}{T}\int_O^T t^n dt$$

$$= n\lambda_{DU}^n\left[\frac{t^n}{n}\right]_O^T - \lambda_{DU}^n\frac{n}{T}\left[\frac{t^{n+1}}{n+1}\right]_O^T$$

$$= \{\lambda_{DU}T\}^n - \{\lambda_{DU}T\}^n\frac{n}{n+1}$$

$$= \{\lambda_{DU}T\}^{n}\left(1-\frac{n}{n+1}\right)$$

$$= \{\lambda_{DU}\ \ T\}^{n}\left(\frac{1}{n+1}\right)$$

$$= \frac{\{\lambda_{DU}T\}^{n}}{n+1}$$

Average probability of functional failure on demand

In condition of Figure 4, average probability of functional failure on demand is

$$PFD_{avg} = \frac{\{\lambda_{DU}T\}^{n}}{n+1} \tag{12}$$

4.2. Calculation of hazardous or harmful event rate

It is derived from hazardous or harmful event rate of 1-out-of-n system to PFD_{avg}.

That is

an average probability F(t) of system fault in proof test(0, T], when demand occurs during (0, T] by event rate λ_M .

$$PFD_{avg} = \int_O^T F(t)^n\ \lambda_M\, dt$$

$$= \lambda_M \int_O^T \{\lambda_{DU}t\}^{n}\ dt$$

$$= \lambda_M\ \{\lambda_{DU}\}^{n}\ \int_O^T t^n dt$$

$$= \lambda_M\ \{\lambda_{DU}\}^{n}\ \left[\frac{t^n}{n+1}\right]_O^T$$

$$= \lambda_M\ \{\lambda_{DU}\}^{n}\left(\frac{T^{n+1}}{n+1}\right)$$

$$= \lambda_M \{\lambda_{DU}T\}^n\ (T\ /\ n+1) \tag{13}$$

On the other hands,

$$PFD_{avg} = Pr\ \{\text{risk occurs during } (0, T]\ \}\ /\ Pr\{\text{ demand occurs during } (0, T]\ \}$$

$$= \left\{\lambda_M\{\lambda_{DU}T\}^n\ \frac{T}{n+1}\right\}/\{\ \lambda_M T\}$$

$$= \{\lambda_{DU}T\}^n\ /\ (n+1) \tag{14}$$

4.3. Calculation of mean fault time

Mean fault time Tb^* is derived from each PFD_{avg} at clause 4.1. and clause 4.2. .

From formula (10),

$$PFD_{avg} = \{\lambda_{DU}T\}^n \ (T_b^*/T) \tag{15}$$

From formula (12) or formula (14),

$$PFD_{avg} = \frac{\{\lambda_{DU}T\}^n}{(n+1)} \tag{16}$$

From formula (15) and formula (16),

$$\{\lambda_{DU}T\}^n \ \frac{T_b^*}{T} = \frac{\{\lambda_{DU}T\}^n}{(n+1)}$$

In this,

$$T_b^* = T/(n+1) \tag{17}$$

5. SUMMARY

From the result of this paper, mean fault time Tb^* is

$$T_b^* = T/(n+1) \tag{18}$$

It is judged correctly because of same results are derived from two methods, i.e. ,reliability and hazardous or harmful event rate.

When we evaluate safety integrity level correctr, we use a Markov-state transition diagrams.

The mean fault time is useful to modelling of repair of dangerous un-detected failure by a Markov state-transition diagram.

References

[1] IEC 61508, *"Functional safety of electrical / electronic / programmable electronic safety-related systems, Part 1 "*, IEC, Geneva, Dec. 1998 - Feb. 2000.

[2] IEC 61508, *"Functional safety of electrical / electronic / programmable electronic safety-related systems, Part 4 "*, IEC, Geneva, Dec. 1998 - Feb. 2000.

[3] IEC 61508, *"Functional safety of electrical / electronic / programmable electronic safety-related systems, Part 6 "*, IEC, Geneva, Dec. 1998 - Feb. 2000.

[4] Yoshinobu SATO, *"Basis of Functional safety / Machinery Safety standard and Risk assessment - evaluation of SIL, PL, Automotive SIL "*, NIKKAN KOGYO SHIMBUN,LTD. , pp 20-27, Aug. 2011.