

# Quantitative Evaluation on Safety-related Systems

Wei LONG<sup>\*</sup>, Tie Ling ZHANG<sup>\*\*</sup> & Masaki OSHIMA<sup>\*</sup>

<sup>\*</sup> Department of Electronics and Mechanical Engineering  
Tokyo University of Mercantile Marine  
2-1-6 Etchujima, Koto-Ku  
Tokyo 135-8533  
Tokyo  
long@ipc.tosho-u.ac.jp  
oshima@ipc.tosho-u.ac.jp

<sup>\*\*</sup> HAL Corporation  
6-21-17-701 Nishikasai, Edogawa-Ku  
Tokyo 134-0088  
Tokyo  
zhangtling@yahoo.com

## Abstract

Among a number of techniques available to the analysis of safety integrity level for safety-related systems, reliability block diagrams and Markov models are used to evaluate the probability of failure on demand in IEC 61508. However, there are no clear descriptions for some results. It is not easy for a safety engineer to understand the solutions. This paper aims at presenting clue to assessing the capability of safety-related systems by reliability block diagrams.

## 1. Introduction

With the publication and enforcement of IEC 61508 functional safety of electrical/electronic/program electronic safety-related systems (IEC 61508), a recent tendency of development from qualitative towards a quantitative analysis in the fields of reliability and safety has realized. In this standard, two frameworks are concerned: one is risk reduction with safety-related systems and the other is the overall safety lifecycle. The configurations of safety-related systems, proof test, self-diagnostic coverage and the failure rates of components are often utilized in the evaluation of safety integrity levels of safety-related systems. The safety integrity levels of safety-related systems need to be evaluated by quantitative analyses as required by IEC 61508. However, the standard neither prescribes how to perform the analysis nor has clear descriptions for many results, such as average probability of failure on demand of system architectures. It is not easy for a common safety engineer to carry out quantitative analyses.

The present paper deals with the quantitative analyses of the safety-related systems. Their system configurations are composed of channels that include both detectable failures with self-diagnosis and undetectable failures. The reliability block diagrams are applied to evaluating the probabilities of failure on demand. The expected down time  $E(T_1-t)$  for the undetected failure during the interval  $[0, T_1]$  and average failure rate of the system  $\lambda_{sys}$  are introduced in order to evaluate the probabilistic parameters of system architectures. The results with the detailed derivations are given.

## Notation

$t_{cl}$	equivalent mean down time (hour) for the undetected failure of a channel
$t_{CE}$	channel equivalent mean down time (hour) for 1001, 1002, 2002, 2003 architectures
$t_{GE}$	voted group equivalent mean down time (hour) for 1002 and 2003 architectures
$D$	dangerous failure rate of a channel in a subsystem (per hour)
$DD$	detected dangerous failure rate of a channel in a subsystem (per hour)
$DU$	undetected dangerous failure rate (per hour)
$MTTR$	mean time to restoration (hour)
$PF D_G$	average probability of failure on demand for system architectures

## 2. Expected down time $E(T_1-t)$ and average system failure rate $\lambda_{sys}$

According to IEC 61508, system configurations are composed of channels. Each channel can be considered to include two components, one with an undetected failure rate  $\lambda_{DU}$  and the other with a detected failure rate  $\lambda_{DD}$ . Based on the assumptions given in IEC 61508,  $\lambda_{DD}$  and  $\lambda_{DU}$  are constant over the life of the system. For the detected failures with self-diagnosis, they are repaired to be as good as new whereas the undetected failures cannot be detected until the next proof test. Figure 1 shows the detection process for the undetected failures by proof test. Here,  $t$  and  $T_1-t$  are the time of occurrence of the undetected failure during the proof test interval  $[0, T_1]$  and the duration of down time, respectively.

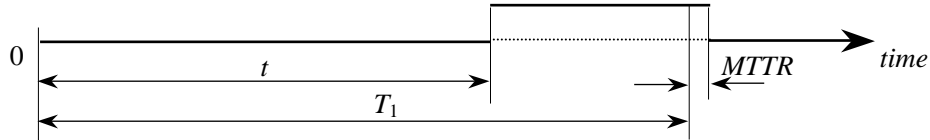


Figure 1: Process for the undetected failures

The expected down time of the undetected failures in a channel during the interval  $[0, T_1]$  can be given by the following equation:

$$E(T_1 - t) = \frac{\int_0^{T_1} (T_1 - t) f(t) dt}{\int_0^{T_1} f(t) dt} = \frac{\int_0^{T_1} (T_1 - t) \lambda_{DU} \exp(-\lambda_{DU} t) dt}{1 - \exp(-\lambda_{DU} T_1)} \approx \frac{T_1}{2} \quad (1)$$

where  $f(t)$  is the probability density function and  $\exp(-\lambda_{DU} T_1) \approx 1 - \lambda_{DU} T_1$  when  $\lambda_{DU} T_1 \ll 1$ . Then,  $t_{c1}$ , the equivalent mean down time of the undetected failure in a channel is

$$t_{c1} = E(T_1 - t) + MTTR = \frac{T_1}{2} + MTTR \quad (2)$$

For the  $m$ -out-of- $n$  redundant safety-related systems (refer to 1oo2 and 2oo3 architectures), the failure probability of a single channel and the failure probability of  $(n-m+1)$  channels during the interval  $[0, T_1]$  are  $\lambda_{DU} T_1$  and  $\binom{n}{n-m+1} (\lambda_{DU} T_1)^{n-m+1}$ , respectively. Figure 2 is the reliability block diagram of the system. Then, the average failure rate of the system during the interval  $[0, T_1]$  can be obtained:

$$\lambda_{sys} = \binom{n}{n-m+1} \frac{(\lambda_{DU} T_1)^{n-m+1}}{T_1} = \frac{n!}{m!(n-m)!} \lambda_{DU}^{n-m+1} T_1^{n-m} \quad (3)$$

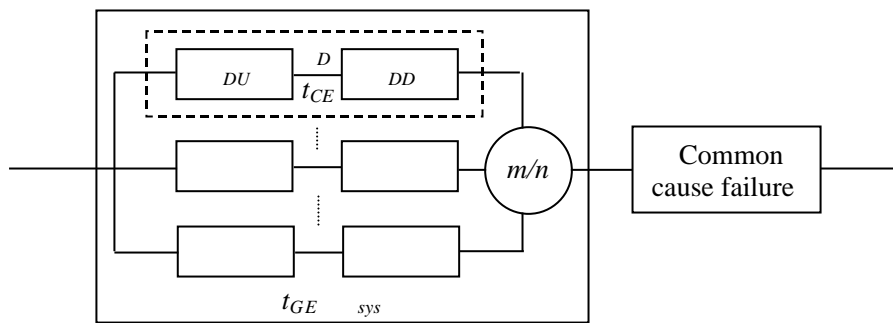


Figure 2:  $m$ -out-of- $n$  safety-related system reliability block diagram

### 3. $PFD_G$ of system architectures

#### 3.1 1001

This system consists of a single channel with two components, where any dangerous failure leads to a failure of the safety function when a demand arises. The channel equivalent mean down time,  $t_{CE}$ , is in direct proportion to each component's contribution to the probability of failure of the channel:

$$t_{CE} = \frac{DU}{D} \left( \frac{T_1}{2} + MTTR \right) + \frac{DD}{D} MTTR \quad (4)$$

For the 1001 architecture, the average probability of failure on demand is

$$PFD_G = ( \quad_{DU} + \quad_{DD} ) t_{CE} \quad (5)$$

#### 3.2 1002

The system consists of two channels connected in parallel. For the 1002 architecture, the system loses the safety function only when both two channels are the failed states. The probability density function,  $f(t)$ , is

$$f(t) = F'(t) = [ ( \quad_{D} t )^2 ]' = 2 \quad_{D}^2 t \quad (6)$$

Then, the expected down time for the undetected failure of the system during the interval  $[0, T_1]$  is

$$E(T_1 - t) = \frac{\int_0^{T_1} (T_1 - t) f(t) dt}{\int_0^{T_1} f(t) dt} = \frac{\int_0^{T_1} (T_1 - t) 2 \quad_{D}^2 t dt}{( \quad_{D} T_1 )^2} = \frac{T_1}{3} \quad (7)$$

Therefore, similar to the equation (4), the system equivalent mean down time is obtained:

$$t_{GE} = \frac{DU}{D} \left( \frac{T_1}{3} + MTTR \right) + \frac{DD}{D} MTTR \quad (8)$$

The average failure rate for the 1002 architecture during the interval  $[0, T_1]$  is given by the equation (3):

$$\lambda_{sys} = \quad_{D}^2 T_1 \quad (9)$$

We know  $t_{CE}$  of one channel approximately equals to  $T_1/2$  for the non-repairable systems. For repairable systems, usually  $T_1 \gg MTTR$ , then  $t_{CE}$  of one channel can be seen to almost equal to  $T_1/2$ . Therefore, the average probability of failure on demand for 1002 architecture is obtained by adding the influence of common cause failures  $P_{CC}$ :

$$\begin{aligned} PFD_G &= \lambda_{sys} t_{GE} + P_{CC} = 2 \quad_{D}^2 t_{CE} t_{GE} + \quad_{D} \quad_{DD} MTTR + \quad_{DU} \left( \frac{T_1}{2} + MTTR \right) \\ &= 2 [ (1 - \quad_{D}) \quad_{DD} + (1 - \quad_{DU}) ]^2 t_{CE} t_{GE} + \quad_{D} \quad_{DD} MTTR + \quad_{DU} \left( \frac{T_1}{2} + MTTR \right) \end{aligned} \quad (10)$$

where  $\quad_{D}$  and  $\quad_{DU}$  are the fraction of detected failures and undetected failures that have a common cause.

### 3.3 2oo3

Similarly, by using the equations (1)~(3), the system equivalent mean down time and average system failure rate are

$$t_{GE} = \frac{DU}{D} \left( \frac{T_1}{3} + MTTR \right) + \frac{DD}{D} MTTR \quad (11)$$

and

$$t_{sys} = 3 \frac{DU}{D} T_1 = 6 \frac{DU}{D} t_{CE} \quad (12)$$

The average probability of failure on demand for the 2oo3 architecture is

$$PFD_G = 6 \left[ (1 - \lambda_D) \lambda_{DD} + (1 - \lambda_{DU}) \right]^2 t_{CE} t_{GE} + \lambda_D \lambda_{DD} MTTR + \lambda_{DU} \left( \frac{T_1}{2} + MTTR \right) \quad (13)$$

### 3.4 2oo2 and 1oo2D

For the 2oo2 architecture, the system loses the safety function when either channel fails. Therefore,  $PFD_G$  is

$$PFD_G = 2 \lambda_D t_{CE} \quad (14)$$

For the 1oo2D architecture, the detected safe failure rate of a channel  $\lambda_{SD}$  is taken into account. By referring to the 1oo2D reliability block diagram given in IEC 61508,  $PFD_G$  can be expressed as

$$PFD_G = 2 \left( 1 - \lambda_{DU} \right) \left[ \left( 1 - \lambda_{DU} \right) + \left( 1 - \lambda_D \right) \lambda_{DD} + \lambda_{SD} \right] t_{CE}' t_{GE}' + \lambda_D \lambda_{DD} MTTR + \lambda_{DU} \left( \frac{T_1}{2} + MTTR \right) \quad (15)$$

where  $t_{CE}'$  and  $t_{GE}'$  are the channel equivalent mean down time and voted group equivalent mean down time for 1oo2D architecture and are given by the following equations respectively.

$$t_{CE}' = \frac{DU \left( T_1 / 2 + MTTR \right) + \left( \lambda_{DD} + \lambda_{SD} \right) MTTR}{DU + \lambda_{DD} + \lambda_{SD}}$$

$$t_{GE}' = \frac{DU \left( T_1 / 3 + MTTR \right) + \left( \lambda_{DD} + \lambda_{SD} \right) MTTR}{DU + \lambda_{DD} + \lambda_{SD}}$$

## 4. Conclusions

The safety integrity levels of safety-related systems need to be quantitatively evaluated by IEC 61508. In the paper, the expected down time for the undetected failure during the interval  $[0, T_1]$  and the system failure rates are newly proposed. The average probabilities of failure on demand that are obtained with the detailed derivation processes are of the same as those presented in IEC 61508. This paper gives clear descriptions for the results given in IEC 61508. It makes possible for a safety engineer to carry out quantitative analyses.

## References

- IEC 61508 (2000), Functional safety of E/E/PE safety-related systems.  
 Shimizu H., Fukuda T. (2000). Machinery safety engineering. Yokendo Ltd. (in Japanese).