# THE IMPROVEMENT OF SIL CALCULATION METHODOLOGY

Jinhyung Park[1]

[1] *Yokogawa Electric Korea: 21, Seonyu-ro45-gil Yeongdeungpo-gu, Seoul, 07209, Jinhyung.park@kr.yokogawa.com*

*Safety Integrity Level (SIL) is applied to prevent plant incident. The most fundamental international standard of Safety Integrity Level is IEC61508. There were also other international standard to describe Safety Integrity Level, but there were some explosion incidents caused by applying the old methodology of Safety Integrity Level. So the sophisticated methodology of Safety Integrity Level is required to prevent the plant explosion incident. For SIL calculation, both of the Hardware Fault Tolerance (HFT) methodology and PFDavg calculation shall be executed and the lower SIL between the result of HFT and the result of PFDavg calculation shall be selected as result SIL. For PFDavg calculation, there are 3 methodologies of Reliability Block Diagram (RBD), Fault Tree Analysis (FTA), Markov Chain, but RBD methodology is most recommended considering the convenience of application. In addition, the Common Cause Failure (Beta Factor) and Proof Test Coverage (PC) shall be included in the formula of PFDavg for more sophisticated SIL calculation. IEC61508 edition 2 are the latest international standard to describe Safety Integrity Level, but the more sophisticated SIL calculation methodology is required for actual project execution.*

## I. INTRODUCTION

In safety lifecycle, the target SIL is determined during risk analysis and the result SIL is calculated during SIS realisation phase. It is regarded as safe only when the result SIL is higher or equal to the target SIL. There are various methodologies to calculate the result SIL. Even though IEC61508 edition 2.0 2010-04 is the latest standard to introduce the result SIL calculation formula, the guideline on IEC61508 is not enough to calculate the result SIL about the instruments in real project. In this paper, the various methodologies to calculate the result SIL will be introduced and the better SIL calculation formula than IEC61508 will be derived.

## II. THE SIL CALCULATION METHODOLOGY ON IEC61508 AND SOME ARGUMENT

It is normally required to calculate the Hardware Fault Tolerance and PFDavg to determine the result SIL. The Hardware Fault Tolerance is required in IEC61508 Part 2 and PFDavg is required IEC61508 Part 1 and Part 6. To obtain the conservative conclusion, the lower SIL between the Hardware Fault Tolerance and PFDavg is determined as the result SIL. Nowadays the consequence of explosion incidents is bigger and bigger because the scale of plants are getting bigger and the number of plants are also increased. Sometimes the explosion incidents are caused by the failure of SIF. Considering this kinds of facts, it is easy to understand the reason why the result SIL shall be concluded in conservative way even though it is hard to find the clear sentence in IEC61508 to say the reason why the lower SIL between the Hardware Fault Tolerance and PFDavg. We also need to consider that all of safety related methodologies recommend the conservative way. During the hazard and risk analysis and the SIL calculation for result SIL, there are many arguments about the detailed methodologies because the clear and detailed guideline about everything are not described in IEC61508. But in most cases, we can get the clear answer if we ask to our internal conscience. It is obvious that we should select the conservative conclusion if the safe case is expected in one result and the incident is expected in the other result, because our conscience always say that the life and environment are more important than economic benefit.

## III. THE HARDWARE FAULT TOLERANCE

### III.A. Hardware Fault Tolerance General Requirement

The meaning of hardware fault tolerance is described in IEC61508 Part 2 as below.

Citation:

7.4.4.1.1 With respect to the hardware fault tolerance requirements

a) a hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function (for further clarification see Note 1 and Table 2 and Table 3). In determining the hardware fault tolerance no accident shall be taken of other measures that may control the effects of faults such as diagnostics: and

b) where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault:

c) when determining the hardware fault tolerance achieved, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem. Any such fault exclusions shall be justified and documented (Ref. 01)

The Hardware Fault Tolerance is recognized as the same meaning as the hardware safety integrity architectural constraints. IEC61508 Part 2 describes the hardware safety integrity architectural constraints as below.

Citation:

7.4.4 Hardware safety integrity architectural constraints

In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be archieved by implementing one of two possible routes (to be implemented at system or subsystem level):

- Route 1H based on hardware fault tolerance and safe failure fraction concepts; or,
- Route 2H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.(Ref. 01)

It is very hard to apply Route 2H because most of end users don't have their own component reliability databook. So usually Route 1H is applied. Even in case that Route 2H is applied, there is no special benefit because finally failure mode is necessary to calculate PFDavg. IEC61508 Part 2 describes Route 1H as below.

Citation:

7.4.4.2 Route 1H

7.4.4.2.1 To determine the maximum safety integrity level that can be claimed, with respect to a specified safety function, the following procedure shall be followed:

1) Define the subsystems making up the E/E/PE safety-related system.

2) For each subsystem determine the safe failure fraction for all elements in the subsystem separately (i.e. on an individual element basis with each element having a hardware fault tolerance of 0). In the case of redundant element configurations, the SFF may be calculated by taking into consideration the additional diagnostics that may be available (e.g. by comparison of redundant elements).

3) For each element, use the achieved safe failure fraction and hardware fault tolerance of 0 to determine the maximum safety integrity level that can be claimed from column 2 of Table 2 (for Type A elements) and column 2 of Table 3 (for Type B elements).

4) Use the method in 7.4.4.2.3 and 7.4.4.2.4 for determining the maximum safety integrity level that can be claimed for the subsystem.

5) The maximum safety integrity level that can be claimed for an E/E/PE safety-related system shall be determined by the subsystem that has achieved the lowest safety integrity level. (Ref. 01)

IEC61508 Part 2 describes Table 2 and Table 3 as below.

**Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem**

| Safe failure fraction of an element | Hardware fault tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60 % | SIL 1 | SIL 2 | SIL 3 |
| 60 % – < 90 % | SIL 2 | SIL 3 | SIL 4 |
| 90 % – < 99 % | SIL 3 | SIL 4 | SIL 4 |
| ≥ 99 % | SIL 3 | SIL 4 | SIL 4 |

(Ref. 01)

**Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem**

| Safe failure fraction of an element | Hardware fault tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| <60 % | Not Allowed | SIL 1 | SIL 2 |
| 60 % – <90 % | SIL 1 | SIL 2 | SIL 3 |
| 90 % – <99 % | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99 % | SIL 3 | SIL 4 | SIL 4 |

(Ref. 01)

### III.B. Type A and Type B

It is very hard for normal engineers to distinguish Type A and Type B in the above Table 2 and Table 3 IEC61508 Part 2 describes Type A and Table B as below.

Citation:

7.4.4.1.2 An element can be regarded as type A if, for the components required to achieve the safety function

a) the failure modes of all constituent components are well defined; and

b) the behaviour of the element under fault conditions can be completely determined; and

c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met

7.4.4.1.3 An element can be regarded as type A if, for the components required to achieve the safety function

a) the failure mode of at least one constituent component is not well defined; or

b) the behaviour of the element under fault conditions cannot be completely determined; or

c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures (Ref. 01)

Even though the definition of Type A and Type B on IEC61508 edition 2 is much more detailed than IEC61508 edition 1, it is still very hard to distinguish Type A and Type B. One of easy methods to distinguish Type A and Type B is to check if microprocessor is installed in the element. Mostly there is microprocessor is installed in Type B element.

### III.C. Safe Failure Fraction

The safe failure fraction (SFF) is described as below in IEC61508 Part 2.

Citation:

Annex C. Diagnostic coverage and safe failure fraction

C.1 Calculation of diagnostic coverage and safe failure fraction of a hardware element

f) For the element, calculate the total dangerous failure rate, ($\Sigma\lambda D$), the total dangerous failure rate that is detected by the diagnostic tests, ($\Sigma\lambda Dd$), and the total dangerous failure rate that is detected by the diagnostic tests, ($\Sigma\lambda S$),

h) Calculate safe failure fraction of the element as :

$$SFF = (\Sigma\lambda s + \Sigma\lambda Dd) / (\Sigma\lambda S + \Sigma\lambda Dd + \Sigma\lambda Du) \text{ (Ref. 01)}$$

### III.D. Reliability Block Diagram

In combination of series elements, the lowest SIL among SIL of all elements is selected as maximum SIL as the below figure.

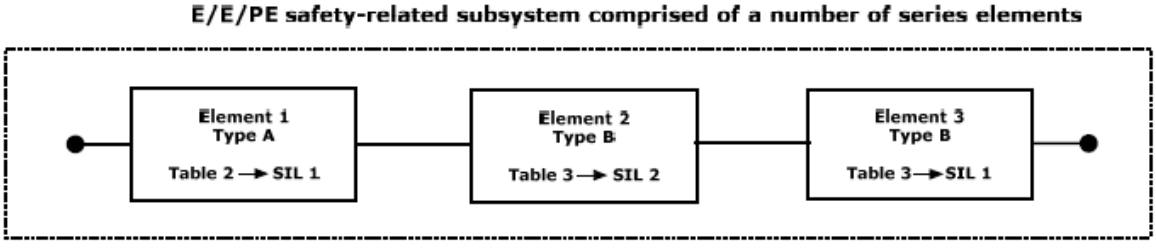


Fig. 1. Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprising a number of series elements) (Ref. 01)

If the architecture of the reliability block diagram is parallel as below figure, the SIL is increased.

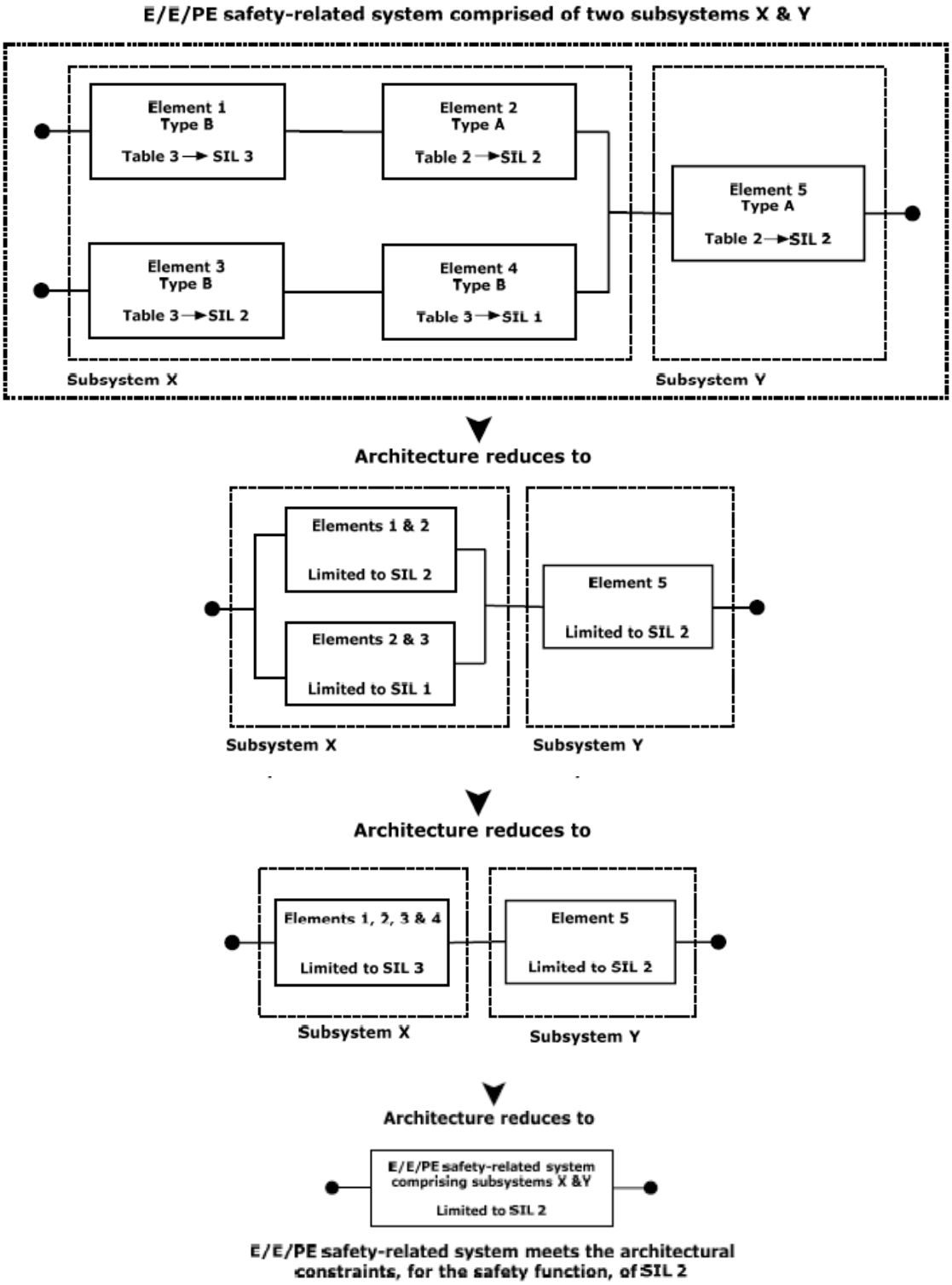


Fig. 2. Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprised of two subsystem X & Y)

In reliability block diagram, one block means that the Hardware Fault Tolerance is 0 and two parallel blocks means that the Hardware Fault Tolerance is 1 and three parallel blocks means that the Hardware Fault Tolerance is 2. So parallel blocks increase SIL. The reliability block diagram (RBD) is introduced in IEC61508 Part 6 as below.

Citation:

B.2 Consideration about basic probabilistic calculations

B.2.1 Introduction

The reliability block diagram (RBD) on Figure B.1 is representing a safety loop made of three sensors (A,B,C), one logic solver (D)m two elements (E,F), and common cause failures (CCF).

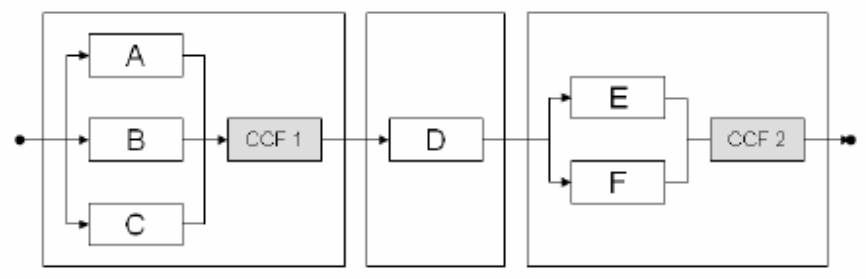


Fig. 3. Reliability Block Diagram of a whole safety loop

This facilitate the identification of five failure combinations leading to the E/E/PE safety-related system failure. Each of them is a so-called minimal cut set:

- (A,B,C) is a triple failure:
- (E,F) is a double failure;
- (D) (CCF1) (CCF2) are single failures. (Ref. 02)

Mostly SIL calculation is executed through the reliability block diagram because the reliability block diagram is the simplest methodology.

## IV. THE OTHER METHODOLOGIES THAN RBD

Sometimes other methodologies than RBD like fault tree and Markovian approach are used to calculate the result SIL.

### IV.A. Fault Tree

The fault tree (FT) is described in IEC61508 Part 6 as below.

Citation:

B.4 Boolean approach

B.4.3 Fault tree model

Fault trees have exactly the same properties as RBD but in addition they constitute an effective deductive (top-down) method of analysis helping reliability engineers to develop models step by from the top event (unwanted or undesirable event) to the individual components failures.

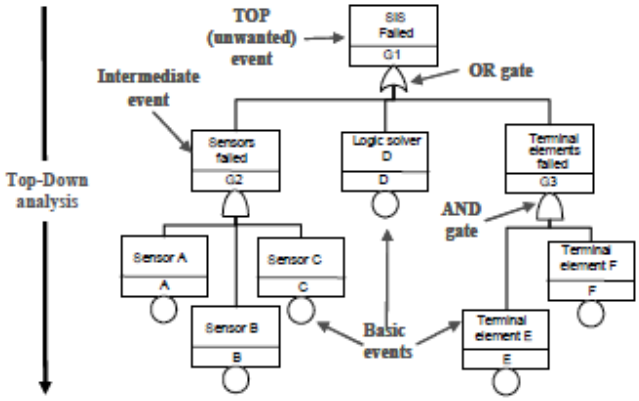


Fig. 4. Simple fault tree equivalent to the reliability block diagram presented on Figure 3

Figure 3 shows a fault tree which is perfectly equivalent to the RBD presented on Figure 3 but where the steps of the top-down analysis are identified (for example: E/E/PE safety-related system failed => Sensor failed => sensor A failed). In FT, the elements in series are linked by “OR gates” and element in parallel (i.e. redundant) are linked by “AND gates”. (Ref. 02)

### IV.B. Markovian Approach

Except Fault Tree, Markovian approach can be used to calculate the result SIL. The Markovian approach is most analytic methodology but is not used normally because it is hard for normal engineer to understand the Markovian approach.

Citation:

B.5.2 Markovian approach

B.5.2.1 Principle of modelling

The Markovian approach is the elder of all the dynamic approaches used in the reliability field. Markov processes are split between those which are “amnesic” (homogeneous Markov processes where all transition rates are constant) and the others (semi Markov processes). As the future of a homogeneous Markov process does not depend on its past, analytical calculation are relatively straightforward. This is more difficult for semi Markov processes for which Monte Carlo simulation can be used. In this part of the IEC61508 series, only homogeneous Markov processes are considered and the term “Markov processes” is used for the sake of simplicity.

The fundamental basic formula of Markov processes is the following:

$$P_i(t+dt) = \sum_{k \neq i} P_k(t)\lambda_{ki}dt + P_i(t)(1 - \sum_{k \neq i} \lambda_{ik}dt)$$

In this formula, λki is the transition rate (e.g. failure or repair rate) from state i to state k. It is self explaining: the probability to be in state i at t+dt is the probability to jump toward i (when in another state k) or to remain in state i (if already in this state) between t and t+dt.

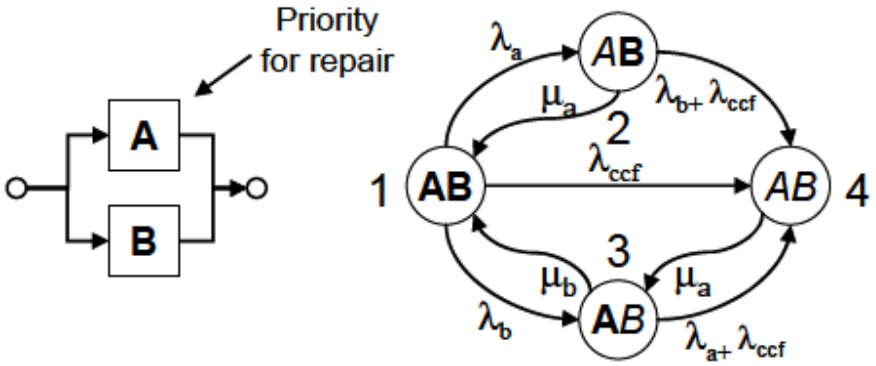


Fig. 5. Markov graph modelling the behavior of a two component system

There is a straightforward relationship between the above equation and a graphical representation like Figure 5 which models a system made of two components with a single repair team (component A having priority to be repaired) and a common cause failure. In this figure A indicates that A is working and A that it has failed. As the detection times must be considered μa and μb in Figure 5 are the restoration rates of the components (i.e. μa =1/MTTRa and μb =1/MTTRb).

For example the probability to be in state 4 is simply calculated as follows:

$$P_4(t+dt) = [P_1(t)\lambda_{ccf} + P_2(t)(\lambda_b + \lambda_{ccf}) + P_3(t)(\lambda_a + \lambda_{ccf})]dt + P_4(t)(1-\mu_a dt)$$

(Ref. 01)

## V. PFD AND PFH

### V.A. PFD General Requirements

The definition of PFD is descibed in IEC61508 Part 4 as below.
Citation:
3.6.17
probability of dangerous failure on demand, PFD
safety unavailability of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system
Note 1 The [instantaneous] unavailability (as per IEC60050-191) is the probability that an item is not in a state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided. It is generally noted by U(t). (Ref. 03)
3.6.18
average probability of dangerous failure on demand
PFDavg
mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system
NOTE 2 Two kind of failures contribute to PFD and PFDavg: the dangerous undetected failure occurred since the last proof test and genuine on demand failures caused by the demands (proof tests and safety demands) themselves. The first one is time dependent and characterized by their dangerous failure rate λDu(t) whilst the second one is dependent only on the number of demands and is characterized by a probability of failure per demand (denoted by γ). (Ref. 03)
3.6.19
average frequency of a dangerous failure per hour
PFH
average frequency of a dangerous failure of an E/E/PE safety related system to perform the specified safety function over a given period of time (Ref. 03)

The application of PFDavg and PFH is described in IEC61508 Part 1 as below.

Citation:

7.6.2.9 When the allocation has sufficiently progressed, the safety integrity requirements, for each safety function allocated to the E/E/PE safety-related system(s), shall be specified in terms of the safety integrity level in accordance with Table 2 or Table 3 ans shall indicate whether the target failure measure is, either:

- the average probability of dangerous failure on demand of the safety function, (PFDavg), for a low demand mode of operation (Table 2), or

- the average frequency of a dangerous failure of the safety function [$h^{-1}$], (PFH), for a high demand mode of operation (Table 3), or

- the average frequency of a dangerous failure of the safety function [$h^{-1}$], (PFH), for a continuous mode of operation (Table 3). (Ref. 04)

**Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation**

| Safety integrity level (SIL) | Average probability of a dangerous failure on demand of the safety function ($PFD_{avg}$) |
|---|---|
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ |

**Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation**

| Safety integrity level (SIL) | Average frequency of a dangerous failure of the safety function [$h^{-1}$] (PFH) |
|---|---|
| 4 | $\geq 10^{-9}$ to $< 10^{-8}$ |
| 3 | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-6}$ to $< 10^{-5}$ |

(Ref. 04)

**V.B. Demand**

The definitions of low demand of operation, high demand of operation and continuous mode of operation are described in IEC61508 Part 4 as below.

Citation:

3.5.16

mode of operation

way in which a safety function operation, which may be either

- low demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or
- high demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
- continuous mode: where the safety function retains the EUC in a safe state as part of normal operation (Ref. 03)

In practice, the dangerous failure of PFDavg and PFH means the dangerous undetected failure. The dangerous detected failure cause the spurious trip and result in protective action. Only the dangerous undetected failure can result in incident among failure modes. The definition of demand is not clearly descibed in IEC61508 but the demand in IEC61508 means that the request for protective action (i.e. pressure high trip, level low trip, spurious trip caused by detected failure, etc)

### V.C. Common Cause Failure Factor

The common cause failure factor (β-factor) and the proof test coverage (PC) shall be included in PFDavg formula. The definition of common failure is described on IEC61508 Part 4 as below.

Citation:

3.6.10

common cause failure

failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure (Ref. 03)

The definition of common failure is also described on IEC61508 Part 6 as below.

Citation:

Common Cause Failure (CCF) causing multiple failures from a single shared cause. The multiple failures may occur simultaneous or over a period of time

Therefore, common cause failures which result from a single cause, may affect more than one channel or more than one component. (Ref. 02)

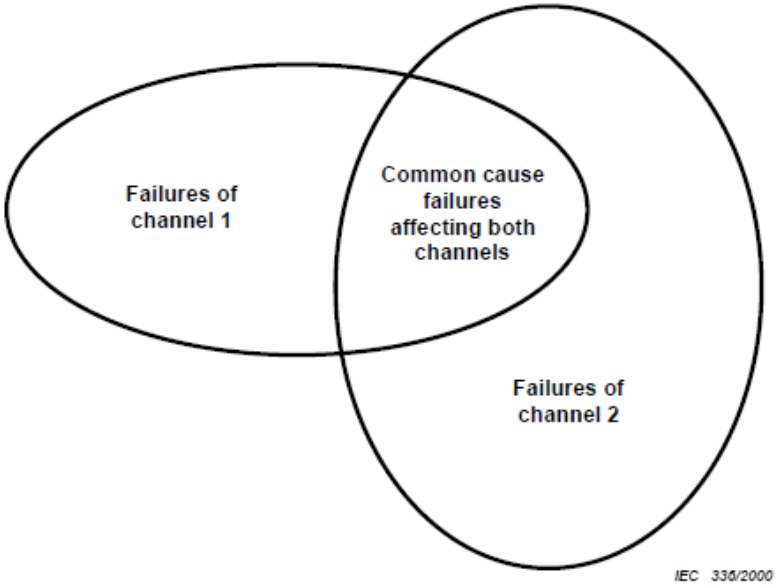


Fig. 6. Relationship of common cause failures

The β-factor is described on IEC61508 Part 6 as below.

Citation:

The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere)

The common cause failure β-factors for the interaction between the channels in the voted group

β is the β-factor in the absence of diagnostic tests, i.e. the fraction of single-channel failures that affect all channels.

β is the common cause failure factor for undetectable dangerous faults, which is equal to the overall β-factor that would be applicable in the absence of diagnostic testing.

The β-factor should be calculated for the sensors, the logic subsystem and the final elements separately. (Ref. 02)

### V.D. Proof Test Coverage

The definition of proof test is described in IEC61508 Part 4 as below.
Citation:
3.8.5
proof test
periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition (Ref. 01)

The proof test coverage (PTC) is described in IEC61508 Part 6 as below.
Citation:
B.3.2.5 Effects of a non-perfect proof test
Faults in the safety system that are not detected by either diagnostic tests or proof tests may be found by other methods arising from events such as a hazardous event requiring operation of the safety function or during an overhaul of the equipment. If the faults are not detected by such methods it should be assumed that the faults will remain for the life of the equipment. Consider a normal proof test period of *T1* where the fraction of faults detected when a proof test is performed is designated as PTC (proof test coverage) and the fraction of the faults not detected when a proof test is performed is designated as (1-PTC). These latter faults which are not detected at the proof test will only be revealed when a demand is made on the safety-related system at demand period *T2*. Therefore, the proof test period (*T1* ) and the demand period (*T2* ) govern the effective down time. (Ref. 02)

### V.E. The improvement of PFDavg formula in IEC61508

PFDavg formula are desciribed on IEC61508 Part 6 edition 2: 2010. One of problems of PFDavg formula on IEC61508 Part 6 edition 2 :2010 is that $\lambda_{Dd}$ is also included in PFDavg formula. $\lambda_{Dd}$ result in spurious trip and protective action by recent fail-safe technology and $\lambda_{Dd}$ does not result in incident. So $\lambda_{Dd}$ should not be included in PFDavg considering this technology development. In addition, PC is not included in the formula on IEC61508 Part 6 edition 2:2010. How to improve PFDavg formula is described in the below.

#### *V.E.1. 1oo1 architecture*

In IEC61508 Part 6 edition 2:2010, 1oo1 reliability block diagram is drawn as below.

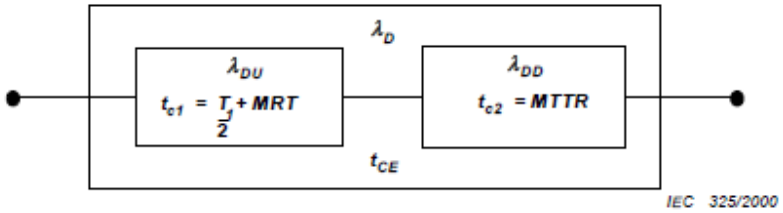


Fig. 7. 1oo1 reliability block diagram (IEC61508) (Ref. 02)

And PFDavg formula for 1oo1 is written as below.

$$PFD_G = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

$PFD_G$: Average probability failure on demand
$t_{ce}$ : Mean down time (Ref. 02)

If we exclude $\lambda_{Dd}$ and include PC, we can improve reliability block diagram and PFDavg formula as below.

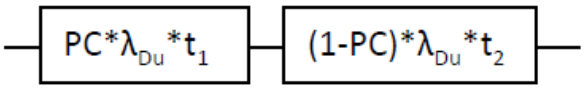


Fig. 8. 1oo1 reliability block diagram (improved)

$$PFD_{AVG} = \left[\tfrac{1}{2} * PC * \lambda_{Du} * T\right] + \left[\tfrac{1}{2} * (1 - PC) * \lambda_{Du} * T_L\right]$$

$t_1$ = T (proof test Interval)

$t_2$ = $T_L$ (lifetime)

T: Proof Test Interval

$T_L$: Life time

*V.E.2. 2oo2 architecture*

In IEC61508 Part 6 edition 2:2010, 2oo2 reliability block diagram is drawn as below.

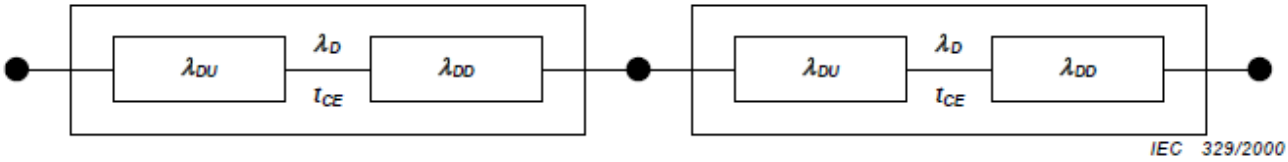


Fig. 9. 2oo2 reliability block diagram (IEC61508) (Ref. 02)

And PFDavg formula for 2oo2 is written as below.

$$PFD_G = 2\lambda_D t_{CE}$$

$PFD_G$: Average probability failure on demand

$t_{CE}$ : Mean down time (Ref. 02)

If we exclude $\lambda_{Dd}$ and include PC, we can improve reliability block diagram and PFDavg formula as below.

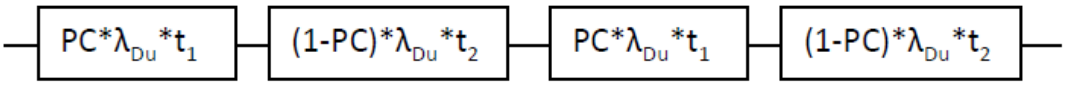


Fig. 10. 2oo2 reliability block diagram (improved)

$$PFD_{AVG} = 2 * \left\{\left[\tfrac{1}{2} * PC * \lambda_{Du} * T\right] + \left[\tfrac{1}{2} * (1 - PC) * \lambda_{Du} * T_L\right]\right\}$$

$t_1$ = T (proof test Interval)

$t_2$ = $T_L$ (lifetime)

T: Proof Test Interval

$T_L$: Life time

*V.E.3. 1oo2 architecture*

In IEC61508 Part 6 edition 2:2010, 1oo2 reliability block diagram is drawn as below.

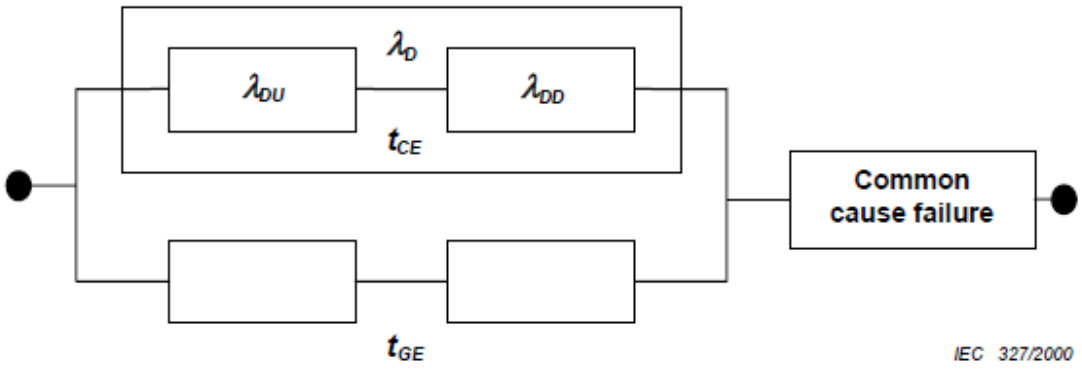


Fig. 11. 1oo2 reliability block diagram (IEC61508) (Ref. 02)

And PFDavg formula for 1oo2 is written as below.

$$PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

$PFD_G$: Average probability failure on demand

$t_{CE}$ : Mean down time

$t_{GE}$ : System equivalent down time

MTTR: Mean Time To Restoration (hour)

MRT: Mean Repair Time (hour) (Ref. 02)

If we exclude $\lambda_{Dd}$ and include PC, we can improve reliability block diagram and PFDavg formula as below.

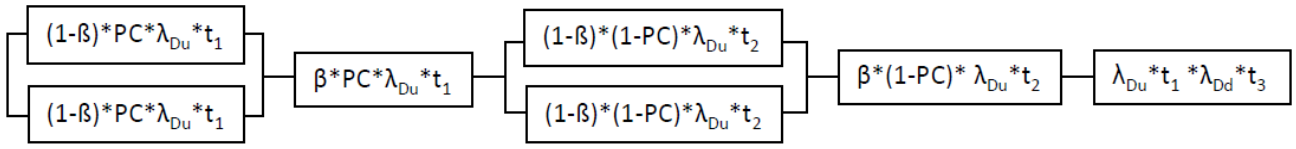


Fig. 12. 1oo2 reliability block diagram (improved)

$$PFD_{AVG} = \left[\tfrac{1}{3} * (1-\beta)^2 * PC^2 * \lambda_{Du}^2 * T^2\right] + \left[\tfrac{1}{2} * \beta * PC * \lambda_{Du} * T\right] + \left[\tfrac{1}{3} * (1-\beta)^2 * (1-PC)^2 * \lambda_{Du}^2 * T_L^2\right] + \left[\tfrac{1}{2} * \beta * (1-PC) * \lambda_{Du} * T_L\right] + \left[\tfrac{1}{3} * \lambda_{Du} * MTTR/T * \lambda_{Dd} * T^2\right]$$

$t_1$ = T (proof test Interval)

$t_2$ = $T_L$ (lifetime)

T: Proof Test Interval

$T_L$: Life time

MTTR: Mean Time To Repair (hour)

*V.E.4. 2oo3 architecture*

In IEC61508 Part 6 edition 2:2010, 2oo3 reliability block diagram is drawn as below.

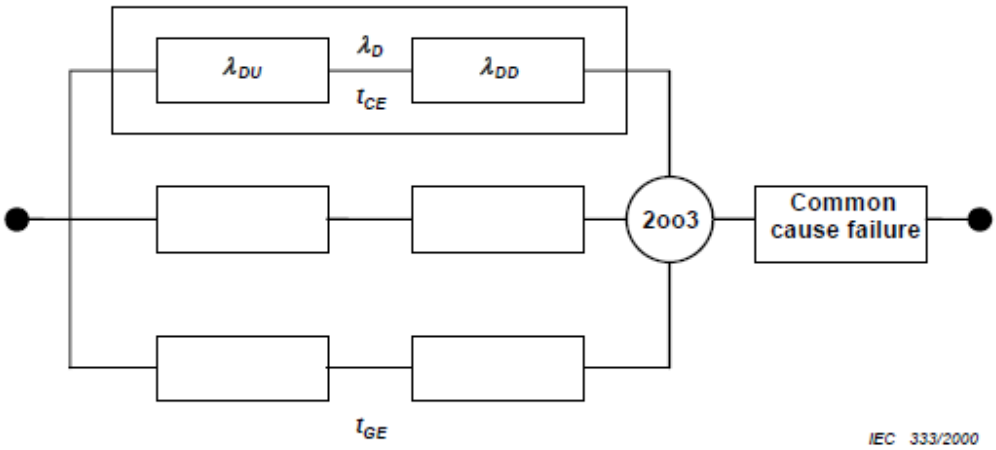


Fig. 13. 2oo3 reliability block diagram (IEC61508) (Ref. 02)

And PFDavg formula for 2oo3 is written as below.

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

PFDG: Average probability failure on demand

$t_{CE}$ : Mean down time

$t_{GE}$ : System equivalent down time
MTTR: Mean Time To Restoration (hour)
MRT: Mean Repair Time (hour) (Ref. 02)

If we exclude $\lambda_{Dd}$ and include PC, we can improve reliability block diagram and PFDavg formula as below.

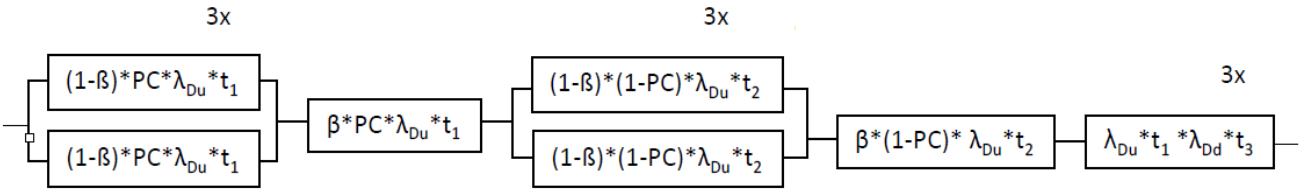


Fig. 14. 2oo3 reliability block diagram (improved)

$$PFD_{AVG} = \left[(1-\beta)^2 * PC^2 * \lambda_{Du}^2 * T^2\right] + \left[\tfrac{1}{2} * \beta * PC * \lambda_{Du} * T\right] + \left[(1-\beta)^2 * (1-PC)^2 * \lambda_{Du}^2 * T_L^2\right] + \left[\tfrac{1}{2} * \beta * (1-PC) * \lambda_{Du} * T_L\right] + \left[\lambda_{Du} * MTTR + \tfrac{1}{T} * \lambda_{Dd} * T^2\right]$$

$t_1$ = T (proof test Interval)

$t_2$ = $T_L$ (lifetime)
T: Proof Test Interval
$T_L$: Life time
MTTR: Mean Time To Repair (hour)

*V.E.5. 1oo3 architecture*

In IEC61508 Part 6 edition 2:2010, PFDavg formula for 1oo3 is written as below

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

PFDG: Average probability failure on demand

$t_{CE}$ : Mean down time

$t_{GE}$ : System equivalent down time
MTTR: Mean Time To Restoration (hour)
MRT: Mean Repair Time (hour) (Ref. 02)

If we exclude $\lambda_{Dd}$ and include PC, we can improve reliability block diagram and PFDavg formula as below.

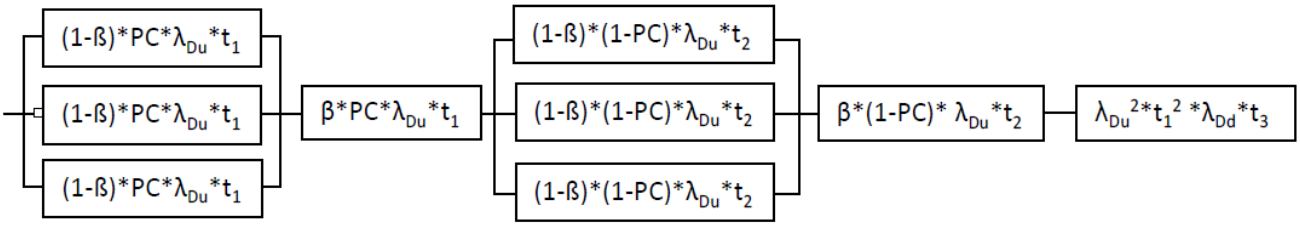


Fig. 15. 1oo3 reliability block diagram (improved)

$$PFD_{AVG} = \left[\tfrac{1}{4}*(1-\beta)^3*PC^3*\lambda_{Du}{}^3*T^3\right] + \left[\tfrac{1}{2}*\beta*PC*\lambda_{Du}*T\right] + \left[\tfrac{1}{4}*(1-\beta)^3*(1-PC)^3*\lambda_{Du}{}^3*T_L{}^3\right] + \left[\tfrac{1}{2}*\beta*(1-PC)*\lambda_{Du}*T_L\right] + \left[\tfrac{1}{4}*\lambda_{Du}{}^2*MTTR/T*\lambda_{Dd}*T^3\right]$$

$t_1$ = T (proof test Interval)

$t_2$ = $T_L$ (lifetime)
T: Proof Test Interval
$T_L$: Life time
MTTR: Mean Time To Repair (hour)

## VI. CONCLUSIONS

It is hard to reflect the every latest technology in International Standard. Until the modification of international standard, the right method shall be developed theoretically and practically. IEC61508 was first issued on 1999 and IEC61508 Edition 2 was issued on 2010, but the PFDavg formula were almost not revised. The next revision of IEC61508 shall contain the new and practical PFDavg formula to prevent the argument and chaos about PFDavg formula. Even though there are many arguments about SIL calculation, the safer and practical SIL calculation methodology shall be continuously developed and applied to prevent the incident by wrong SIL calculation.

## ACKNOWLEDGMENTS

This research work is done as activity of national research project titled “Development of Turret System for FPSO Operating at Hs 15m by the support of Korea Evaluation Institute of Industrial Technology (KEIT). I appreciate the support of KEIT for this research work.

## REFERENCES

1. IEC 61508-4 Edition 2.0 2010-04, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electric/programmable electric safety-related systems
2. IEC 61508-6 Edition 2.0 2010-04, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
3. IEC 61508-4 Edition 2.0 2010-04, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Definition and abbreviations

4. IEC 61508-1 Edition 2.0 2010-04, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements