Potential of Fault-Detection Coverage by means of On-Chip Redundancy - IEC61508: Are There Royal Roads to SIL 4?

Nobuyasu KANEKAWA†(a), Senior Member

SUMMARY This paper investigates potential to improve fault-detection coverage by means of on-chip redundancy. The international standard on functional safety, namely, IEC61508 Ed. 2.0 Part 2 Annex E.3 prescribes the upper bound of $\beta_C$ (common cause failure (CCF) ratio to all failures) is 0.25 to satisfy frequency upper bound of dangerous failure in the safety function for SIL (Safety Integrated Level) 3. On the other hand, this paper argues that the $\beta_C$ does not necessarily have to be less than 0.25 for SIL 3, and that the upper bound of $\beta_C$ can be determined depending on failure rate $\lambda$ and CCF detection coverage. In other words, the frequency upper bound of dangerous failure for SIL 3 can also be satisfied with $\beta_C$ higher than 0.25 if the failure rate $\lambda$ is lower than 400 [fit]. Moreover, the paper shows that on-chip redundancy has potential to satisfy SIL 4 requirement; the frequency upper bound of dangerous failure for SIL 4 can be satisfied with feasible ranges of $\beta_C$, $\lambda$ and CCF coverage which can be realized by redundant code.

key words: on-chip redundancy, fault-detection, common cause failure, functional safety, IEC61508

1. Introduction

The logic gate count within one chip is continuously being enhanced by the progress of the miniaturization according to Moore’s Law [1]; accordingly, nowadays, a whole processor system can be constituted within one chip. With further advances of miniaturization, it is possible to constitute plural systems within one chip. As a result, a multi-core processor constituting plural processor cores within one microprocessor chip has become commercially available.

It has been commonly supposed that a single event upset (SEU) is induced by an alpha ray emitted from radioisotopes used in package/packaging materials. Moreover, in 1996, it was predicted that an SEU is induced in computer memory by cosmic rays in the memory on the ground level [2]. Nowadays, an SEU induced by cosmic rays (in particular, secondary cosmic rays generated by collision of atoms of the atmosphere with neutron from galaxy) has become a realistic problem at ground level [3].

In previous studies, to realize self-checking or fail-safe LSIs, on-chip redundancy (namely, redundant subsystems within a chip for detecting error), self-checking comparator and optimal time diversity techniques [4] were proposed, and a prototype LSI was fabricated [5], [6]. In addition, safety microcontrollers have been commercially launched by several vendors [7], [8].

Fault-detection coverage is the key issue in on-chip redundancy and greatly depends upon the independence of fault occurrence among the redundant subsystems, and the fault-detection coverage of comparison mechanism.

As for fault-detection coverage with on-chip redundancy, IEC61508 Ed. 2.0 [9] Part 2 Annex E introduces $\beta_C$ as a coefficient of proportion of undetectable failure due to CCF (Common Cause Failure) to all failures in a semiconductor chip with on-chip redundancy. However, the standard provides descriptions just like a royal road only for SIL 3. It is wise to make the descriptions more balanced to include not only SIL (Safety Integrity Level) 3, but also SIL 4. To promote development of science and technology, it is preferable to extend and to apply IEC61508 Ed. 2.0 mutatis mutandis (with necessary modification) for SIL 4 certification of systems using on-chip redundancy before revising the standard.

Many studies related to interpretation and usage of IEC61508 (Ed.1.0) were accomplished; Zhang et al. proposed formulation on availability of systems having safety related system with self diagnosis function [10]. Fujiiwara et al. proposed the definition method of the safety of the software for the operation demand of high-frequency or continuous modes and the calculation method [11]. And Panesar-Walawege et al. proposed a conceptual model on software safety based on the standard [12]. But not so many studies related to IEC61508 Ed.2.0 were accomplished because it was established recently.

This paper investigates potential of fault detection by means of on-chip redundancy and shows that on-chip redundancy has potential to satisfy SIL 4 requirement.

In this paper, IEC61508 is outlined in Sect. 2, ratio of CCF in the case of on-chip redundancy is explained in Sect. 3, discussion on fault-detection coverage by means of on-chip redundancy in Sect. 4, supplemental CCF countermeasures such as code theoretical protection and hybrid on-chip redundancy techniques are proposed in Sect. 5.

2. Functional Safety Standard IEC61508*

IEC61508, “Functional safety of electrical/electronic/ programmable electronic safety-related systems” is an international standard on functional safety stipulated in 2000 by IEC.

*Due to copyright issue, this paper does not show text or table as it is in IEC61508. The standard is available from IEC Webstore; http://webstore.iec.ch/
The term “functional safety” is proposed as an antonym of conventional “inherent safety” or “intrinsic safety”. There are various opinions on its definition, and the standard defines it as an approach to define an allowable safety level and to ensure the defined allowable safety level is achieved by adding an artificial countermeasure to a target device.

“Safely-related systems” means emergency stop functions and they were often installed independently of the main body of the targeted machine when the standard was established. As inferred by the words “programmable electronic,” however, in the case of recent microprocessors, the function of “safely related systems” and the original functions of the targeted machine are realized together.

In years of late, the safety of electronic systems must be assured, and the terms “SIL 2” and “SIL 3” still appear in various documents. SIL is the level of safety defined by IEC61508. The SIL that a safely-related system should satisfy is classified in SIL 1-4 according to the incidence and severity of the harm by the failure of a device. The probability of a dangerous failure on demand and frequency of a dangerous failure of the safety functions for SIL 1-4 are defined. Table 1 shows an example of the frequency of dangerous failure definitions for each SIL.

In addition, IEC61508 prescribes a normative procedure for safety for the entire 16 phases of lifecycles (from the conceptual planning stage to the modification, maintenance and repair, and disposal phases).

A probabilistic approach has conventionally been taken for such safety-related rules. However, in years of late, a deterministic approach (namely, prescribing a methodology for procedures and techniques for design and testing to secure safety) is largely employed. This is because the probabilistic approach required many samples for inspection and failure-rate prediction. In addition, the deterministic approach fits the human sense more than the probabilistic approach based on the law of large numbers because an individual human has only one life.

The scope of this standard covers devices that could have a major influence on human life in case of failure; accordingly, it includes a great deal of industrial applications of devices in modern society. Right after the establishment of IEC61508, in 2001, IEC61513 (covering the field of atomic energy) was established, and as shown in Fig. 1, a functional safety standard for each application field was established in sequence. IEC61508 is therefore referred as an upper-level standard among these field standards. In addition, a functional-safety microcomputer especially for automotive-control applications has been launched by several semiconductor companies.

IEC61508 was revised as Edition 2.0 in 2010, namely, ten years after its establishment, and consists of seven parts described as follows [1].

Part 1: General requirements
Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
Part 3: Software requirements
Part 4: Definitions and abbreviations
Part 5: Examples of methods for the determination of safety integrity levels
Part 6: Guidelines on the application of IEC61508-2 and IEC61508-3
Part 7: Overview of techniques and measures

The following major revisions are added to Ed. 2.0:

- Functional Safety Management Methodology
- Recommendations on Security
- Issues on Digital Communications
- Standards for ASIC, Integrated Circuits, and On-Chip Redundancy
- Requirements for Qualitative Risk Assessment of Software
- Change and Addition of Terminology

3. Ratio of CCF in Case of On-Chip Redundancy

Failure or fault events are classified in mutually exclusive and collectively exhaustive manner as Fig. 2. Failure occurrence classified into two categories, namely, CCF and non-CCF (i.e., independent cause failure). Each failure is classified as “detected” or “undetected”. The undetected failures become dangerous failures in the safety functions.

IEC61508 defines $\beta_{CC}$ as the ratio of undetected CCFs to all failures, but hereinafter it is defined as the ratio of CCFs without considering detected or undetected. In addition, detection coverage for non-CCF is defined as C, and that for CCF is defined as $C_{CCF}$. The standard is defined above under the assumption that $C_{CCF}$ is zero; namely, all
CCFs are undetectable. As shown by Fig. 2, incidence rate of each failure event is expressed in terms of $\beta IC$, $C$ and $C_{CCF}$. Because the fault-detection mechanism has an influence in case of CCF, $C_{CCF}$ is generally smaller than $C$.

Incidence rate of undetectable failure $\lambda D$ is expressed using $\beta IC$ as

$$\lambda D = \lambda D_{NCCF} + \lambda D_{CCF} = \lambda (1 - \beta IC)(1 - C) + \lambda \beta IC(1 - C_{CCF})$$

where,

- $\lambda D_{NCCF}$: Failure rate of undetectable non-CCF
- $\lambda D_{CCF}$: Failure rate of undetectable CCF
- $\lambda$: Failure rate of item,
- $C$: Coverage of the fault-detection mechanism, and
- $C_{CCF}$: Coverage of the fault-detection mechanism in case of CCF.

Here, coverage $C$ depends on the type of fault-detection mechanism and generally ranges from 0.6 to 0.99. If fault-detection by comparing duplicated subsystems is employed, the coverage $C$ will be in the order of 0.9 or 0.99. All the CCFs are not always undetectable, but it is reasonable that the rate of detection coverage supposes with zero for the worst case because the failure detection function is often implemented inside the chip.

Therefore, if $C \approx 1.0$ and $C_{CCF} \approx 0$ are supposed, the approximation corresponds with the equation stated by IEC61508 Ed.2.0 Part 2 Annex D is obtained,

$$\lambda D \approx \lambda D_{CCF} = \beta IC \lambda$$

(2)

$\lambda D_{CCF}$ is plotted against $\lambda$ for various $\beta IC$ values (0.50, 0.33, and 0.25) in Fig. 3, and $\lambda D_{CCF}$ is plotted against $\beta IC$ when $\lambda$ is 10, 50, 100, 200 and 400 [fit] in Fig. 4 (fit: Failures In Time or Failure unIT $= 1 \times 10^{-9}$/hr.).

IEC61508 Ed. 2.0 Part 2 Annex E.3 prescribes the upper bound of $\beta IC$ as 0.25 for SIL 3. However, if a fault-detection mechanism such as self-checking comparator with redundant code output is employed, as shown by Fig. 5, $C_{CCF}$ can be increased because the soundness of the detection mechanism is guaranteed by the redundant code output. In other words, if the fault-detection mechanism is designed to output code word when duplicated functional blocks agree, a non-code word output represents the disagreement of duplicated functional blocks or unsoundness of the fault-detection mechanism.

Table 2 lists aliasing probability $P_a$ by means of the redundant code. It is necessary to avoid a coding method (for generating a polynomial) that generates a singular code word with all zeros because a singular code word would not detect a CCF due to a power-supply blackout.

In general, aliasing probability $P_a$ by means of the redundant code is expressed as,

$$P_a = N_{CW}/N$$

(3)

where,

- $N_{CW}$: Number of code words, and
Table 2  Aliasing probability and coverage.

<table>
<thead>
<tr>
<th>Redundant code</th>
<th>$P_a$</th>
<th>$C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parity</td>
<td>$1/2$</td>
<td>$1/2$</td>
</tr>
<tr>
<td>Two-rail logic</td>
<td>$1/2$</td>
<td>$1/2$</td>
</tr>
<tr>
<td>SECDED code (6 bit for 16 bit data)</td>
<td>$2^n$</td>
<td>0.98</td>
</tr>
<tr>
<td>General redundant code (n: # of additional bits)</td>
<td>$2^n$</td>
<td>$1-2^n$</td>
</tr>
<tr>
<td>Alternating signal</td>
<td>$1/3$</td>
<td>$2/3$</td>
</tr>
<tr>
<td>Frequency logic</td>
<td>$N_f/N_c$</td>
<td>$1-N_f/N_c$</td>
</tr>
</tbody>
</table>

$N$: Number of all possible words, or

$$P_a = 2^{-n} \quad (4)$$

where, $n$: number of additional redundant bits.

It is also reasonable to assume that the aliasing probability $P_a$ by means of alternate signal output is 1/3 and coverage $C$ is 2/3 assuming that the incidence probability of each failure mode, namely, stuck-at-H, stuck-at-L, and phony alternating signal output, is the same (1/3). The probability of a phony alternating signal output is extremely low in reality and the specific frequency of the alternating signal is granted as good like frequency logic, therefore, the coverage $C_{CCF}$ can be in the order of 0.9 or 0.99.

Assuming that frequency distribution of phony alternating signal is flat, the probability of aliasing $P_a$ by means of frequency logic which is generally used for train control systems is expressed as

$$P_a = N_{fc}/N_f \quad (5)$$

Where,

$N_{fc}$: Number of frequency bands granted as code words,

$N_f$: Number of all possible frequency bands, or

$$P_a = B_{fc}/B_f \quad (6)$$

Where,

$B_{fc}$: Bandwidth of frequency bands for code words, and

$B_f$: Bandwidth of all possible frequency bands.

The possible occurrences of CCFs are explained by a mutually exclusive and collectively exhaustive schematic in

![Fig. 5](image_url)  Fault-detection mechanism with redundant code output.

Fig. 6  CCF events.

$$C_{CCF} = \alpha C_{FDM} + (1-\alpha)(1-\gamma) \quad (7)$$

$C_{CCF}$ plotted against $\alpha$ and $\gamma$, when $C_{FDM}$ = 0.67, and $C$ = 0.99, in Fig. 7.

As shown in the Fig. 7, $\alpha$ varies from 0 to 1.0 and $\gamma$ varies from 0 to 1.0. Moreover, $\gamma$ can be reduced by means of redundant code output employed for the duplicated functional blocks as $\gamma (1-P_a)$ where $P_a$ is probability of aliasing of redundant code output as shown by Table 2. $C_{CCF}$ is 1 when $\alpha$ is 0, and $C_{CCF}$ is $C_{FDM}$ when $\alpha$ is 1.0. In other words, $C_{CCF}$ is no less than $C_{FDM}$ for any $\alpha$ if $C_{FDM} < (1-\gamma)$. In this case the internal fault-detection mechanism works as canary logic which detects CCF by its failure.

In Eq. (1), $\lambda_{D,NCCF}$ is not negligible because $\lambda_{D,CCF}$ becomes comparably small with increased $C_{CCF}$ of the fault-
detection mechanism with redundant code output. It is therefore not possible to use Eq. (2) to determine $A_D$ in the case of improved CCF-detection coverage. $A_D$ plotted against $\lambda$, when $\beta_{IC}$ is 0, 0.25, 0.33 and 0.5, and $C_{CCF}$ is 0, 0.67, 0.9 and 0.99, in Fig. 8.

The figure and Eq. (1) show that $A_D$ satisfies the upper bound for SIL4 (100 [fit] or $1 \times 10^{-8}$ [/hr.]) with likely ranges of $\beta_{IC}$ (0.25-0.5) and $\lambda$ (tens to hundreds [fit]), when $C_{CCF}$ > 0.67.

5. Supplemental CCF Countermeasures

5.1 Code-Theoretical Protection

Employment of code-theoretical protection such as redundant code output and alternate signal output is proposed in this section as a substitute for physical protection.

A method of physical protection such as separation of signals and power/ground lines between redundant functional blocks is generally used and recommended in IEC61508 to mitigate CCFs and to reduce $\beta_{IC}$.

The input port to a fault-detection mechanism (such as a comparator) is the weakest point from the viewpoint of avoidance of connection or intersection of the signals between redundant functional blocks. The possibility of short-circuit or crosstalk is the highest there because it is the closest point of the signal lines from redundant functional blocks. Interconnection between separated blocks (e.g., redundant functional blocks and a comparator) needs an isolator that can transfer information but it is isolated in case of power supply (ground) separation. A fault-detection mechanism such as a comparator is indispensable to realize a self-checking processor using on-chip redundancy (comparing dual processor cores on chip). The effect of a physical protection method has a natural limit. The possible CCFs for redundant functional blocks without power supply/ground separation are a CCF by noise or voltage fluctuation and a CCF by blackout. The former CCF can be mitigated by time diversity and the latter CCF can be mitigated by code theoretical protection as stated above. The author previously proposed a self-checking comparator with an orthogonal function and an alternate signal output [4], and an optimal time diversity to operate redundant functional blocks with time difference of half clock or its odd multiple [4]. The effect of the optimal time diversity was verified by fault injection experiments; that is, it eliminates incidence of CCFs caused by power supply noise [13], [14]. Note that we must avoid the coding method (generating polynomial) that generates singular code word with all 0 because the singular code word does not detect CCF by power supply blackout.

5.2 Classification of On-Chip Redundancy

“On-chip redundancy” is not defined in detail in the standard. Accordingly, following three classes of “on-chip redundancy” are proposed; “full-on-chip redundancy”, “semi-on-chip redundancy” and “hybrid on-chip redundancy” (see Fig. 9). A system with “full-on-chip redundancy” has a fault-detection mechanism such as a comparator, output response analyzer, and collator inside the chip, a system with “semi-on-chip redundancy” has one outside, and a system with “hybrid on-chip redundancy” has ones both inside and outside the chip.

Incidence rate of undetectable failure by means of semi-on-chip redundancy $A_{DS}$ is expressed as

$$A_{DS} = A_{D-NCCF} + A_{D-CCF} = \lambda(1 - \beta_{IC})(1 - C_s) + A_{IC}(1 - C_{CCF_x}) \quad (8)$$

where

$C_s$: coverage of external fault-detection mechanism, and

$C_{CCF_x}$: coverage of external fault-detection mechanism in case of CCF.

$C_{CCF_x}$ is determined by ratio of coincidence of functional block outputs $\gamma$ as,

$$C_{CCF_x} = C(1 - \gamma) \quad (9)$$

Note that $\gamma$ can be reduced by redundant code as indicated in Table 2.
If fault-detections of internal and external fault-detection mechanisms are statistically independent, the incidence rate of undetectable failure in case of hybrid on-chip redundancy $\lambda_{DH}$ is expressed as

$$\lambda_{DH} = \lambda_{D-NCCF} + \lambda_{D-CCF}$$

$$= \lambda (1 - \beta_{IC})(1 - C)(1 - C_x)$$

$$+ \lambda \beta_{IC} (1 - C_{CCF})(1 - C_{CCFx})$$

(10)

In reality, fault-detections of internal and external fault-detection mechanism are dependent because the same techniques are usually employed for fault-detection such as self-checking and diversity techniques. If the fault detections are mutually dependent, an undetected fault by one detection mechanism is overlapped with undetected fault by another fault detection mechanism at the worst case, as shown in Fig. 10 (b). In other words, a fault which cannot be detected by one detection mechanism will also cannot be detected by another detection mechanism.

Therefore, $(1 - C) (1 - C_x)$ should be $\min \{ (1 - C), (1 - C_x) \}$, and $(1 - C_{CCF})(1 - C_{CCFx})$ should be $\min \{ (1 - C_{CCF}), (1 - C_{CCFx}) \}$ for the worst case estimation which is useful in practice, hence follows that

$$\lambda_{DH} = \lambda (1 - \beta_{IC}) \min \{ (1 - C), (1 - C_x) \}$$

$$+ \lambda \beta_{IC} \min \{ (1 - C_{CCF}), (1 - C_{CCFx}) \}$$

(11)

The incidence rate of undetected failure in case of the semi, full and hybrid on-chip redundancy methods when $\lambda = 100$ [fit], $\beta_{IC} = 0.25$, $C = C_x = 0.99$, $C_{FDM} = 0.67$ and $\alpha = 0.5$ are shown in Fig. 11. Moreover, the upper bound and the lower bound of $\lambda_{D}$ and $\lambda_{DH}$, are shown in Figs. 12 and 13, respectively. If $\lambda = 50$ [fit], the incidence rate of undetected failure is half of the Figs. 11, 12 and 13, and satisfies SIL 4 requirement in most of cases.

Incidence rates of undetected failure in case of full, semi and hybrid on-chip redundancy are expressed by Eqs. (1), (8) and (11), respectively. $C_{CCF}$ is expressed by $\alpha$ and $\gamma$ in Eq. (7) and Fig. 7. $C_{CCFx}$ is expressed in Eq. (9) and is equivalent to $C_{CCF}$ in Eq. (7) and Fig. 7 when $\alpha = 0$. Therefore if $(1 - \gamma) < C_{FDM}$, $C_{CCFx} < C_{CCF}$, or $(1 - C_{CCF}) < (1 - C_{CCFx})$, in other words, $\lambda_{D} < \lambda_{DS}$. The internal fault-detection mechanism works as canary logic to detect a CCF by influence to itself in this case. In addition, the hybrid on-chip redundancy and the full-on-chip redundancy have advantage in fault-detection latency over semi on-chip redundancy. An on-chip internal fault-detection mechanism can operate as fast as the duplicated functional blocks but the external fault-detection mechanism operate slower because of signal delay between the duplicated functional blocks and the external fault-detection mechanism.

From the above-mentioned evaluation, it is clear that the hybrid on-chip redundancy is superior to the semi and
full on-chip redundancy in fault-detection coverage and latency. Table 3 summarizes fault-detection latency and coverage of the semi, full and hybrid on-chip redundancy methods.

6. Concluding Remarks

IEC61508 Ed. 2.0 Part 2 Annex E.3 prescribes the upper bound of $\beta\text{IC}$ is 0.25 for SIL 3. On the contrary, this paper presented that the $\beta\text{IC}$ does not necessarily have to be less than 0.25 for SIL 3, and that the upper bound of $\beta\text{IC}$ can be determined depending on failure rate $\lambda$ and CCF detection coverage. It was shown that the upper bound of undetected CCF rate (tightly related to frequency of dangerous failure in the safety function) for SIL3 (100{fit} or $1 \times 10^{-7}$ [hr.]) can be satisfied with $\beta\text{IC}$ higher than 0.25 if the failure rate $\lambda$ is lower than 400{fit}. It was also shown that the upper bound of undetected CCF rate for SIL4 (10{fit} or $1 \times 10^{-8}$ [hr.]) can also be satisfied with lower $\beta\text{IC}$ and lower $\lambda$. In addition, as for the fault-detection coverage in case of CCF, it was shown that the upper bound of undetected CCF rate for SIL4 can be satisfied with a reasonable and likely ranges of $\beta\text{IC}$ (0.25-0.5) and $\lambda$ (tens to hundreds [fit]), when $C_{\text{CCF}}>0.67$, and that $C_{\text{CCF}}>0.67$ can be satisfied by employing redundant code.

Supplemental CCF countermeasures not stated in IEC61508, defined as “code theoretical protection” here (namely, redundant code output, and alternate signal output), were proposed as substitutes for physical protection. In addition, on-chip redundancy was classified as three kinds, and it was shown that a protection method based on hybrid on-chip redundancy has an advantage over methods based on semi and full on-chip redundancy in terms of fault-detection coverage and latency.

Therefore, it is reasonable to apply IEC61508 Ed. 2.0 mutatis mutandis for SIL4 certification; the upper bound of $\beta\text{IC}$ for each SIL should be determined in accordance with $\lambda$, and the frequency of dangerous failure can be reduced by supplemental countermeasures stated in this paper.

Acknowledgements

The author thanks the member of Hitachi, Ltd. for their advices in pursuing research on safety systems.

References


Nobuyasu Kanekawa received the B.E., M.E., and D.E. degrees from Tokyo Institute of Technology in 1985, 1987 and 1997, respectively. During 1991-1992, he stayed in Dept. of Computer Science, UCLA as a visiting scholar. His research interests include dependable computing systems, and his major publication is “Dependability in Electronic Systems”, ISBN 978-1-4419-6714-5, Springer (2010). He is currently Chief Researcher, Hitachi Research Laboratory, Hitachi, Ltd, a member of IFIP TC. 10, WG. 10.4, IEC61508 maintenance team, respectively, Vice Chair of TC. on Dependable Computing, IEICE of Japan, and Director of Reliability Engineering Association of Japan. He will be Program Co-chair of PRDC 2014, Singapore.