Analysis on the application of on-chip redundancy in the safety-critical system

Bai-gen Cai[1], **Cheng-ming Jin**[1a)], **Lian-chuan Ma**[1], **Yuan Cao**[1], **and Hideo Nakamura**[2]

[1] *The School of Electronic and Information Engineering, Beijing Jiaotong Univeristy, Beijing 10044, China*

[2] *The Department of Electronic and Computer Science, College of Science and Technology, Nihon University, Funabashi-shi 274–8501, Japan*

a) *13111045@bjtu.edu.cn*

Abstract: IEC 61508-2010 puts special limits on the on-chip redundancy of one single chip, for example the safety integrity level (SIL) is limited up to SIL 3. About this, however, there are no specific explanations. Based on the safety-critical system of on-chip redundancy for a typical programmable logic device (FPGA), this paper proves that the highest SIL is 3; analyses the factors that may impact the safety integrity of redundancy system, and furthermore, provides reasonable solutions. The results show that the use of 1oo2 channel redundancy scheme can effectively improve the safety integrity level of the on-chip redundancy.

Keywords: on-chip redundancy, the safety-critical system, safety integrity level (SIL), reliability

Classification: Electron devices, circuits, and systems

References

[1] R. Girardey, M. Hübner and J. Becker: IEEE Annual Symposium on VLSI (2010) 469. DOI:10.1109/ISVLSI.2010.11

[2] R. Mariani and P. Fuhrmann: IEEE International Symposium on DFTVS (2007) 123.

[3] International Electrotechnical Commission: IEC 61508 Second Edition: Functional Safety of Electrical/Electronic/Programmable Electronic Systems[S]. Geneva: IEC (2010).

[4] S. Hauge, S. Håbrekke and M. A. Lundteigen: Reliability Prediction Method for Safety Instrumented Systems PDS Example collection [R]. Norway: SINTEF (2010).

[5] P. Hokstad, S. Håbrekke, M. A. Lundteigen and T. Onshus: Use of the PDS Method for Railway Applications[R]. Norway: SINTEF Technology and Society (2009) 15.

[6] ALTERA: Reliability Report 55 1H (2013) http://www.altera.com/literature/rr/rr.pdf.

[7] P. Hokstad, A. Maria and P. Tomis: IEEE Trans. Reliab. **55** (2006) 18. DOI:10.1109/TR.2005.858095

DOI: 10.1587/elex.11.20140153
Received February 21, 2014
Accepted March 24, 2014
Publicized April 17, 2014
Copyedited May 10, 2014

1 Introduction

There are strict requirements for the reliability and safety of Safety-Critical Systems. To improve the system safety, the redundant structural design is usually adopted. Due to that the on-chip redundancy of ASIC designs, such as FPGA, has unique advantages in the economy and size aspects [1, 2], it is widely applied in railway signaling systems. However, the 2010 edition of IEC 61508-2 clearly states that “At the present state of the art, knowledge and experience, it is not feasible to consider and take measures against all effects related to said element (single IC) to gain sufficient confidence for SIL 4” [3]. Although SIL 3 is declared, the complete analysis of common cause failures for on-chip redundancy is still in need.

The existence of common cause failures severely restricts the on-chip redundant systems in enhancing safety integrity levels, and an incomplete common cause failure analysis causes the designer to estimate optimistically the system safety of on-chip redundancy. Therefore, a study on a new method, which is easy to implement in design and can solve the problem successfully, is required. The aim of the paper is to develop an easily implemented method that can solve the problem.

2 Safety integrity index analysis of the architecture of on-chip redundancy

Due to the complexity, the on-chip redundancy of one single chip is normally integrated by two processors. And according to the number of data safety comparator (1 or 2), it can be regarded as 1oo1 or 1oo2 architecture, which is specified in the IEC 61508 standard. As the simplest configuration, 1oo1 architecture, with zero hardware fault tolerance (HFT), it does not meet the requirement of IEC 61508 that the HFT should be greater than zero. Thus, the redundant system of a single chip using 1oo1 architecture cannot reach SIL 4. The following analysis will discuss only the single chip on-chip redundancy based on the 1oo2 architecture.

This article adopts the PDS [4] method, developed by Norwegian Industrial Technology Research Institute (SINTEF), to calculate the average frequency of dangerous failure (PFH), intending to quantify the safety integrity level indicators. PDS method is similar to the calculation method mentioned in IEC 61508-6, but it emphasizes more on common cause failures considerations. In the view of the characteristics of safety-critical systems, the dangerous undetected failure rate (λ_{DU}) is the core, therefore, the impact of dangerous detected failure rate (λ_{DD}) on PFH is not considered in the solution process.

For the fail-safe requirements of the safety-critical system, it adopts the 1 out of 2 architecture, which includes comparison units. The common on-chip redundant safety-critical computer control system is shown in Fig. 1, which consists of two identical channels. Each channel is mainly composed by the input, the processor, the safety output, the comparer and safety clock modules. Additionally, in order to further improve the safety of the output,

© IEICE 2014
DOI: 10.1587/elex.11.20140153
Received February 21, 2014
Accepted March 24, 2014
Publicized April 17, 2014
Copyedited May 10, 2014

the feedback module will be increased, which puts the output action back to the input module in order to determine whether the action is correct.

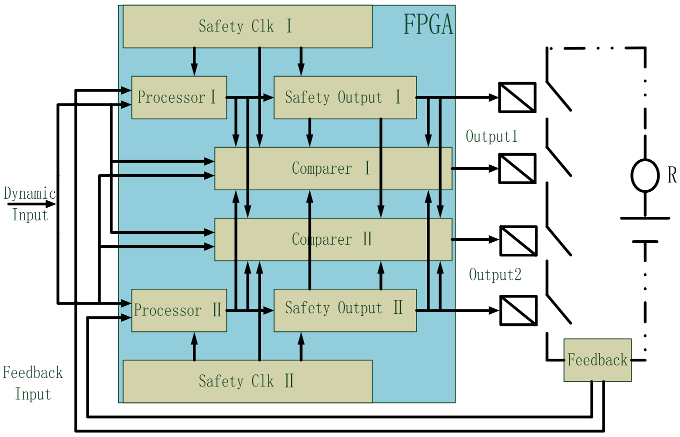

Fig. 1. The schematic diagram of a 1oo2 on-chip redundancy architecture system.

More generally, without considering the impact caused by the modules followed (such as feedback module) on PFH value of the system, according to the system schematic shown in Fig. 1, the reliability block diagram (RBD) of the system can be obtained as Fig. 2. The chip power failure can clearly lead to the system failure, so the safety power is connected in series in the reliability diagram. When two safety clocks fail at the same, the system will fail, and they are shown connected in parallel in the block diagram of the system reliability. Similarly, comparators and processors are structured in parallel. In Fig. 2, white boxes represent that each module is in independent failure and shaded boxes represent common cause failures (CCF) of parallel modules [5].

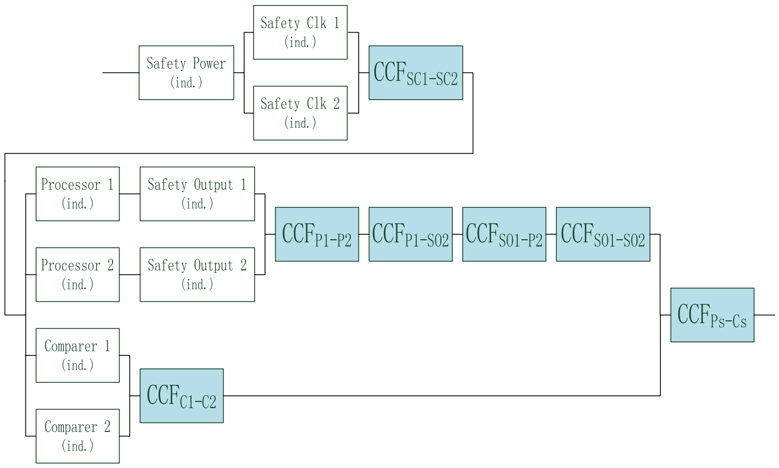

Fig. 2. RBD of 1oo2 system.

According to the RBD, two processors constitute the 1 out of 2 architecture and its PFH value considering the CCF is defined as $PFH_{Processor}$, while two comparators constitute 1 out of 2 and its PFH value considering the CCF

© IEICE 2014
DOI: 10.1587/elex.11.20140153
Received February 21, 2014
Accepted March 24, 2014
Publicized April 17, 2014
Copyedited May 10, 2014

is defined as $\mathrm{PFH}_{\mathrm{Comparer}}$. Meanwhile, the processors and comparators constitute the 1 out of 2 architecture and its PFH value considering the CCF is defined as PFH_{1oo2}. Therefore, the PFH value of system in Fig. 2 is calculated as follows:

$$PFH_{1oo2}^{(\mathrm{IND})} = [(PFH_{\mathrm{Pr}ocessor}) * \tau * (PFH_{Comparer}) * \tau]/\tau \tag{1}$$

The calculation of common cause failures for redundant channels is as follows:

$$\begin{aligned} PFH_{1oo2}^{(\mathrm{CCF})} &= [C_{1oo6}^{*} * \Pr(\mathrm{safe}|1\ \mathrm{nor}) + C_{2oo6}^{*} * \Pr(\mathrm{safe}|2\ \mathrm{nor}) + \mathrm{C}_{3oo6}] \\ &\quad * \beta_{IC} * (\sqrt[3]{\lambda_{DU,\mathrm{Comparer}} * \lambda_{DU,\mathrm{Processor}} * \lambda_{DU,\mathrm{Safety\ Output}}}) \end{aligned} \tag{2}$$

The channel containing dual processors is a dual CPU redundant architecture, so this channel PFH is calculated as follows:

$$\begin{aligned} PFH_{\mathrm{Pr}ocessor} &= [(\lambda_{DU,\mathrm{Pr}ocessor1} + \lambda_{DU,\mathrm{Safety\ Output1}}) * \tau * (\lambda_{DU,\mathrm{Pr}ocessor2} + \lambda_{DU,\mathrm{Safety\ Output2}}) * \tau]/\tau \\ &+ \beta_{IC} * \left(\begin{array}{l} \sqrt{\lambda_{DU,\mathrm{Pr}ocessor1} * \lambda_{DU,\mathrm{Pr}ocessor2}} + \sqrt{\lambda_{DU,\mathrm{Pr}ocessor1} * \lambda_{DU,\mathrm{Safety\ Output2}}} \\ + \sqrt{\lambda_{DU,\mathrm{Safety\ Output1}} * \lambda_{DU,\mathrm{Pr}ocessor2}} + \sqrt{\lambda_{DU,\mathrm{Safety\ Output1}} * \lambda_{DU,\mathrm{Safety\ Output2}}} \end{array} \right) \end{aligned} \tag{3}$$

Another redundant channel containing dual comparators is a redundant architecture, so the channel PFH is calculated as follows:

$$\begin{aligned} PFH_{Comparer} &= [(\lambda_{DU,Comparer1}) * \tau * (\lambda_{DU,Comparer2}) * \tau]/\tau \\ &+ \beta_{IC} * \sqrt{(\lambda_{DU,Comparer1})(\lambda_{DU,Comparer2})} \end{aligned} \tag{4}$$

Where $C_{\mathrm{moon}}^{*} = C_{(\mathrm{m}+1)\mathrm{oon}} - C_{\mathrm{moon}}$, and Pr(safe|x nor) indicates the unfaulty probability of the system, when there are x normal modules. The calculation of PFH value of redundancy chip is shown as follows:

$$PFH_{Chip} = PFH_{SafetyPower} + PFH_{SafetyClk}^{(\mathrm{IND})} + PFH_{SafetyClk}^{(\mathrm{CCF})} + PFH_{1oo2}^{(\mathrm{IND})} + PFH_{1oo2}^{(\mathrm{CCF})} \tag{5}$$

Taking the FPGA of Altera Corporation as an example, the FPGA chip reliability report [6] shows that the chip failure rate λ is at the magnitude of 10^{-8} [h^{-1}], and thus it obviously meets the SIL 4 index requirement when two chips constitute a redundant architecture. At the same time, to form a complete system, the discrete devices in the periphery of redundant chip needs to increase. Compared with ASIC such as FPGA, this kind of the capacitance resistance and other components in general have higher failure rates.

3 Solution

To improve the PFH value of on-chip redundancy for a single chip, the common practice is using components with higher reliability, increasing the fault detection frequency and improving the system's redundancy. The first and second methods usually cannot be widely implemented due to practical conditions (such as economic factors, etc). A promising solution it to take the original on-chip redundant system (1oo2 redundant architecture) as a channel of a higher level of redundancy (1oo2 redundancy) so that the contribution of external discrete devices to the PFH value of the whole system is weakened.

The reliability diagram using 1oo2 redundant channel architecture is shown in Fig. 3. $\mathrm{CCF}_{\mathrm{Device}}$ represents the contributions of common cause

DOI: 10.1587/elex.11.20140153
Received February 21, 2014
Accepted March 24, 2014
Publicized April 17, 2014
Copyedited May 10, 2014

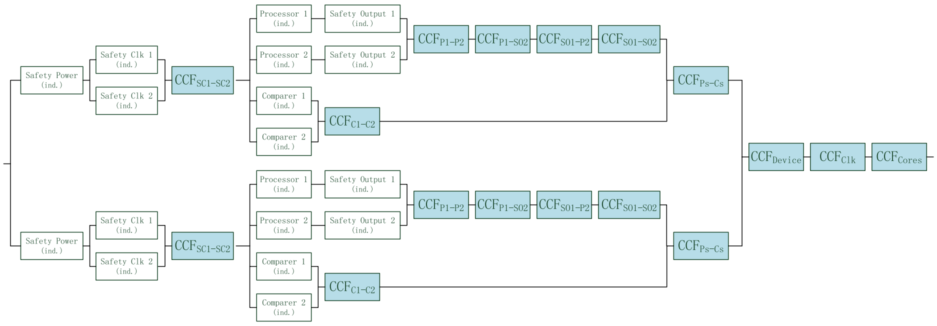

Fig. 3. RBD of 1oo2 system.

failures of two periphery discrete devices to system PFH, $\mathrm{CCF}_{\mathrm{Clk}}$ represents the contributions of common cause failures of two safety clocks (including crystal oscillator unit) to system PFH, $\mathrm{CCF}_{\mathrm{Cores}}$ represents the contributions of common cause failures of two processors, comparisons, and output units to system PFH. The $\mathrm{C}_{\mathrm{Moon}}$ configuration factor values of different redundant architectures are shown in reference [7].

The calculation of PFH value of new redundancy systems is as follows:

$$PFH^{(\mathrm{IND})}_{ChannelA} = PFH^{(\mathrm{IND})}_{\mathrm{ChannelB}} \tag{6}$$

$$PFH^{(\mathrm{CCF})}_{\mathrm{Device}} = \mathrm{C}_{1\mathrm{oo}2} * \beta_{IC} * \lambda_{DU,\ \mathrm{IndependentDevice\&SafetyPower}} \tag{7}$$

$$PFH^{(\mathrm{CCF})}_{\mathrm{Clk}} = \mathrm{C}_{1\mathrm{oo}4} * \beta_{IC} * \lambda_{DU,\ \mathrm{Oscillator\&SafetyClk}} \tag{8}$$

$$\begin{aligned} PFH^{(\mathrm{CCF})}_{Cores} &= \begin{bmatrix} C^{*}_{1\mathrm{oo}12} * \Pr(\mathrm{safe}|1\ \mathrm{nor}) + C^{*}_{2\mathrm{oo}12} * \Pr(\mathrm{safe}|2\ \mathrm{nor}) + \\ C^{*}_{3\mathrm{oo}12} * \Pr(\mathrm{safe}|3\ \mathrm{nor}) + C^{*}_{4\mathrm{oo}12} * \Pr(\mathrm{safe}|4\ \mathrm{nor}) + \mathrm{C}_{5oo12} \end{bmatrix} \\ &* \beta_{IC} * \left(\sqrt[3]{\lambda_{DU,\ \mathrm{Comparer}} * \lambda_{DU,\ \mathrm{Processor}} * \lambda_{DU,\ \mathrm{SafetyOutput}}}\right) \end{aligned} \tag{9}$$

$$\begin{aligned} PFH = {} & [PFH^{(\mathrm{IND})}_{\mathrm{ChannelA}} * \tau * PFH^{(\mathrm{IND})}_{\mathrm{ChannelB}} * \tau]/\tau + \\ & PFH^{(\mathrm{CCF})}_{\mathrm{Device}} + PFH^{(\mathrm{CCF})}_{Clk} + PFH^{(\mathrm{CCF})}_{Cores} \end{aligned} \tag{10}$$

When the quantized residual chip failure rate is 10^{-8}/h and the failure rates of periphery discrete components sum to $501.661 * 10^{-9}$/h, the impact of the higher level redundancy on improving the system SIL is shown below, where DC represents diagnostic coverage. Fig. 4 shows that the PFH value of FPGA chips using 1oo2 redundant architecture satisfies the requirements of SIL 4. Fig. 5 indicates that the PFH value of the entire system using 1oo2 redundant architecture and containing the periphery discrete components can't meet the requirements of SIL 4 (it is impossible that the diagnostic coverage for a complex system is 99% at present). Fig. 6 shows a system adopting the 1oo2 redundant architecture and containing the periphery discrete components. If using 1oo2 redundancy again, its PFH value easily meets SIL 4 requirements.

On-chip redundancy is a typical application of the safety-critical system and this paper analyzes the challenges of on-chip redundancy implemented in the safety-critical system. The conclusions are as follows:

(1) In the 2010 edition IEC 61508-2 for the on-chip redundancy system, limiting the highest safety integrity level to 3 is reasonable. Additionally,

DOI: 10.1587/elex.11.20140153
Received February 21, 2014
Accepted March 24, 2014
Publicized April 17, 2014
Copyedited May 10, 2014

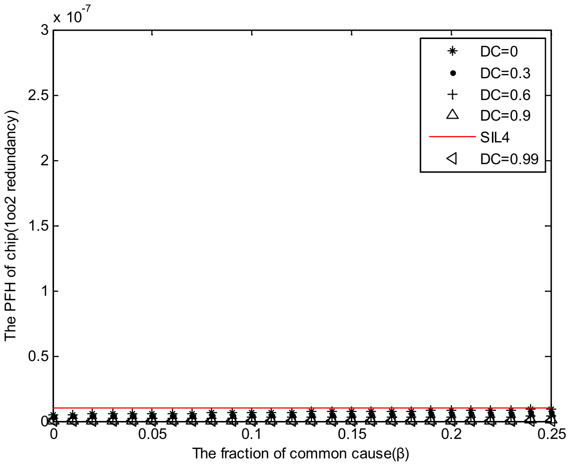

Fig. 4. The PFH of chip (1oo2 redundancy).

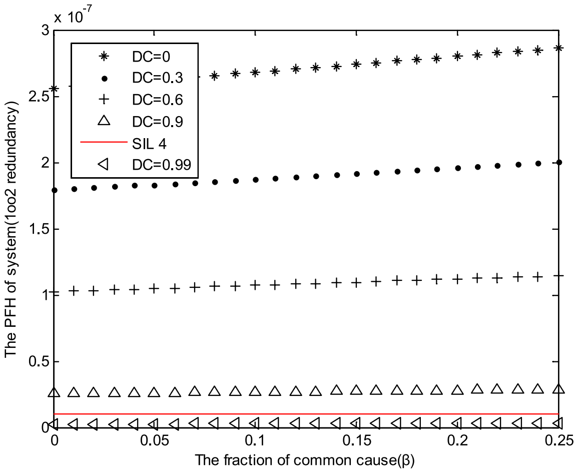

Fig. 5. The PFH of system (1oo2 redundancy).

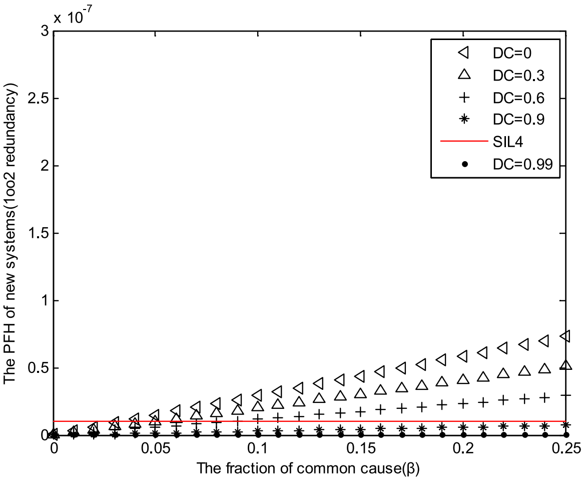

Fig. 6. The PFH of new system (1oo2 redundancy).

© IEICE 2014
DOI: 10.1587/elex.11.20140153
Received February 21, 2014
Accepted March 24, 2014
Publicized April 17, 2014
Copyedited May 10, 2014

improving the reliability of various system units and other index including diagnostic coverage are very important;

(2) Adopting the higher level redundant architecture benefits in solving the problem that system PFH value is affected by chip peripheral discrete devices and further reduces the system PFH value to a predetermined range of SIL 4. However, common cause failures brought by redundancy would put limitations on the improving of safety performance.

4 Conclusions

In this paper, we discuss the safety integrity feature of one single chip redundant system, and propose a reasonable design to effectively improve the safety integrity level (SIL) of one single chip redundant system. Through quantitative indicators, we verify that this proposal can effectively increase PFH value of the overall system to SIL 4 and has high practical value. Therefore, we expect that it will be applied in various applications.

Acknowledgments

This work was supported by the National High Technology Research and Development Program (The 863 program) (2012AA112801), Central university basic research and operating expenses of special funding (2012JBZ014), China Railway Corporation science and technology development plan (2013X013-D), Natural Science Foundation of China (51305021 and U1334211).

DOI: 10.1587/elex.11.20140153
Received February 21, 2014
Accepted March 24, 2014
Publicized April 17, 2014
Copyedited May 10, 2014