Diversity Diagnostic for new FPGA Based Controller of Renewable Energy Power Plant

Kenichi Morimoto*‡, Yuichiro Shibata*, Yudai Shirakura*, Hidenori Maruta*, Masaharu Tanaka*, Fujio Kurokawa**

*Nagasaki University, 1-14, Bunkyo-machi, Nagasaki, 852-8521 Japan

(bb52215205@ms.nagasaki-u.ac.jp)

**Nagasaki Institute of Applied Science, 536, Aba-machi, Nagasaki, 851-0193 Japan

(kurokawa_fujio@nias.ac.jp)

‡Corresponding Author; Kenichi Morimoto 1-14, Bunkyo-machi, Nagasaki, 852-8521 Japan

bb52215205@ms.nagasaki-u.ac.jp

Received: August.28.2017 Accepted: September.1.2017

Abstract- The renewable energy plants tend to require the performance improvement and the scale extension continuously, and also tend to be installed in inconvenient locations for maintenance. Under these background, the control systems of them require high reliability and maintenance-free. In recent years, from the view point of heat generation and system inheritability, the construction of the control system with FPGA (Field Programmable Gate Array) is focused. To design the control system, redundancy with diversity is expected to be the key function to improve reliability and safety of the control, under the consideration of reduction of development cost and production cost. This paper proposes a methodology to generate diverse FPGA circuitries by the Technology-Mapping without both algorism diversity and code diversity. The diversity of the redundant control system is realized by different circuit structures in FPGA with the Technology Mapping and prove-in-use tools. From the simulation of real FPGA implementation setting, it is clarified that the diverse pair of FPGA circuitries improves the error detection rate and the common cause failure fraction. Moreover, it is also clarified that the proposed methodology provides the improvement of MTBF and Safety Integrity level (SIL) of control systems. Therefore, it is revealed that the proposed methodology realizes the new FPGA controller which is suitable for the redundant control system in renewable energy plants.

Keywords FPGA; Diversity; Reliability; Redundancy; Technology Mapping; Functional Safety.

1. Introduction

In order to increase the proportion of renewable energy of total power production, it is necessary to increase the number of such renewable power plants on inconvenient locations. The off-shore wind turbine is a good example of renewable energy power technology which is installed far away from the urban area [1]. In such remote locations, the control systems of renewable energy plants shall be free from frequent and regular maintenance because of the lower accessibility for engineers.

Another aspect is that the renewable energy control systems are getting to require more computation burden for arithmetic processing of control [2][3][4]. The recent operation clock frequency per CPU core is limited up to 2 GHz, and the achievement of higher performance needs to be realized by the multi-core system. Therefore, high-speed multi-core CPUs [5][6] are selected for renewable energy-control systems, instead of simple PLC [7][8]. In order to apply multi-core CPUs in the real time control, complicated middle ware, such as real-time OS, and virtualizing technology for the core are required [9][10]. They also cause the further requirement of higher computation performance. In addition to the problem of computation performance, CPUs generate huge heat when it becomes high performance. It is clear that the system multiplexing amplifies the heat problem. To address the problem of heat, a regular maintenance of cooling devices is required, however, it prevents entire system to be free from maintenance.

It is possible to resolve the above problems of CPU by applying FPGA to the control system. FPGA has specific features such as parallel processing, scalable product selection

and so forth, which CPU cannot provide. Moreover, the recent development of FPGA can realize the capability to use it in the real using situation. For example, the recent FPGA realizes reduction of heat generation as it is advancing year by year and its processing capacity is getting improved dramatically. In addition to the above, the architecture of FPGA is simple and it does not require complicated middle-wares. FPGA logics are easily inherited over generations of devices. These characteristics provide huge advantages to the control systems of long-term operated infrastructures. Hence, control systems configured by FPGA draw considerable attentions [11]-[21]. It is highly provable on renewable energy control systems that the random hardware failures will occur by exposure of stresses from environment, such as noises, temperature and voltage variances of power source.

Figure 1 shows system failures classified by causes. From IEC 61508 Functional Safety [22], the standards of system reliability evaluation for industrial process control and failures causing unreliability are categorized into two factors as shown in Fig. 1. One is a random failure, mainly occur physically in hardware and its elements. Noise influences and softerrors also cause this random failure, as well as degradation of elements [25]. The other is a systematic failure, mainly occur from design faulty or programming errors (e.g. coding errors). In the industrial process controls, high reliable, redundant and fault tolerant systems are required for a long term operation [23]-[26]. FPGA parallel processing mechanism is expected to amplify the efficiency of system diversity as well as it improves the system reliability effectively [27].

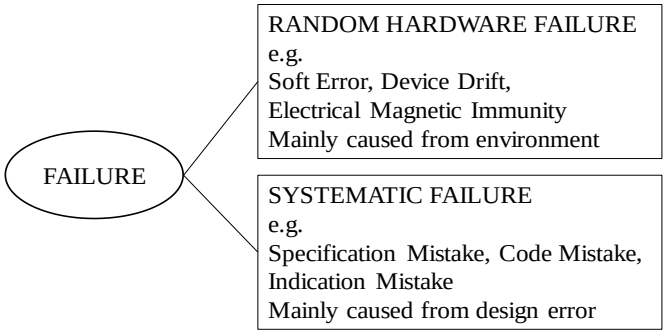


Fig.1. Classification of Failures.

The failure in shared elements is defined as a common cause failure [22]. When the reliability is focused, redundant systems need to consider commonly caused failures in sub-systems. Since the common cause failures occur in redundant sub-systems simultaneously and they cause the entire system failure. For example, when a common grand wire is shared by sub-systems, noise from the common grand wire disables all sub-systems. The Common cause failures are generated from both random hardware failures and systematic failures shown in Fig. 1. Since the systematic failures can be reduced by the effort to improve the quality of implementation of sub-systems, however, it is impossible to avoid the random hardware failures by the effort in the implementation. Therefore, the mainly focused problem is the random hardware failure in this paper.

Renewable energy control systems which are exposed to phenomenal stresses, contain huge risks of common cause failures from random hardware failures. Diversification techniques can reduce the common cause failures and improve reliability of systems [28][29]. Diversification techniques can be realized by three different approaches which are algorithm, code, and hardware diversification[30]. These approaches increase development and production costs, and prevent the implementation of diversification approaches in renewable energy systems. Therefore, another approach is required for the diversification.

This paper proposes a new methodology which realizes diversification of FPGA circuitry based on Technology Mapping of FPGA. The proposed methodology generates FPGA controllers with diverse circuitry and provides the diversification of FPGA circuitry without the diverse techniques of algorisms or codes. The proposed method can make diversity in the appearance of the random hardware errors. Therefore, common cause failures of redundant circuitries are able to be reduced. As a result, this approach realizes the new FPGA controller as an alternative to CPU based one. Since this methodology uses the "proven-in-use" analysis software tool which is used in the world, it is the best suited methodology to the industrial control system; e.g. the renewable energy plant control system.

This paper is organized as follows; Section 2 explains requirements of diversification brought from MTBF and common cause failures of redundant systems. Section 3 explains actual method in realization of diversifications. In Section 4, the proposed method evaluated and effects of it to MTBF is discussed. Section 5 gives conclusion and further studies.

2. MTBF and Common Cause Failures

2.1. Common Cause Failures

Generally, the control system for the power plant is realized as a repairable and redundant system. Therefore, it can be mathematically described as Markov Model. Figure 2 shows the reliability model of redundant systems which considers the common cause failures. Sub-systems are redundant and its failure models are in parallel.

Common cause failures and the failure models are in series since one of the common cause failures leads to the entire system failures. In Fig. 2, λ_{sub_sys} is defined as a sub-system failure rate and β factor is a common cause failure fraction between sub-system controller A and sub-system controller B. As shown in Fig. 2, the reliability improvement by diversification requires β factor common cause failures rate factor to be minimized.

2.2. Markov Model and MTBF of Redundant System without Common Cause Failures

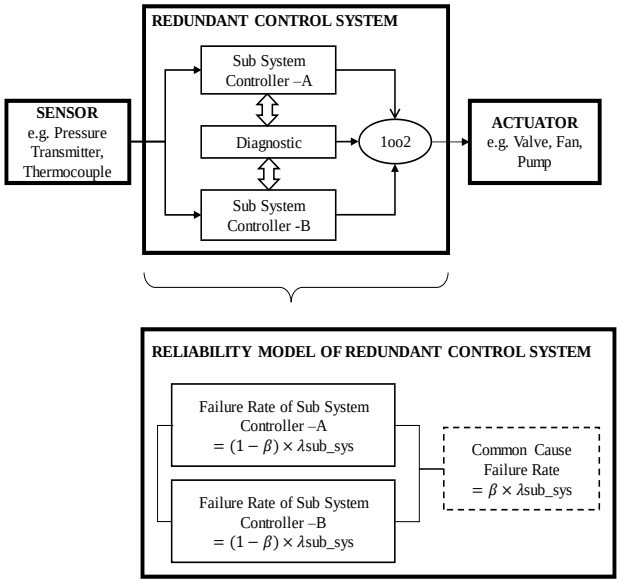
Mean Time Between Failure (MTBF) is the average interval between systems fall into failure. Improvement of availability of renewable energy control systems, and making the maintenance interval longer, equally mean improvement of its MTBF. Figure 3 shows the Markov Model of reparable redundant systems shown in Fig. 2. The common cause failure

is not considered in this model. This Markov Model provides the following MTBF (see Appendix in detail).

$$\text{MTBF} = \frac{1}{2\times\lambda_{sub\_sys}{}^{2}} \quad (1)$$

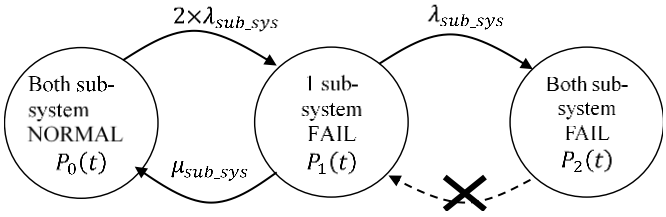
where λ_{sub_sys} is the failure rate of a sub-system (1/hr).

λ_{sub_sys} takes a small value such as 10^{-4} in sub-systems of general industrial controllers[22]. From Eq. (1), MTBF of this model becomes very long about 108 hours (10,000 years) when λ_{sub_sys} is 10^{-4}.



λsub_sys : Failure rate of subsystem
β : Common cause failure rate factor

Fig.2. Reliability Model of Redundant System.



λ_{sub_sys} : The failure rate of a sub-system (1/hr)
μ_{sub_sys} : Repairer Rate of sub-system (1/hr)
$P_0(t)$: Probability of both sub-system is in normal
$P_1(t)$: Probability of 1 sub-system is in fail
$P_2(t)$: Probability of both sub-system are in fail

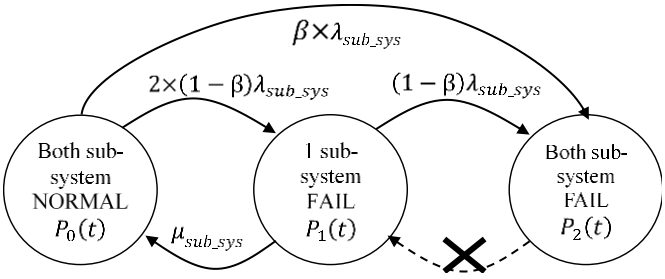
Fig.3. Markov model of duplex system without common cause failure.

2.3. Markov Model and MTBF of Redundant System with Common Cause Failures

MTBF shown in Eq. (1) does not consider the common cause failure, however, the common cause failure is very important for the reliability of the control system as mentioned before. Following issues are considered as common cause failures of redundant systems; common clock drift, quality degradation of supply power (lower voltage), quality degradation of element material (chemically degrading). The FPGA arithmetic is performed by signal transmission in the internal circuitry. For example, the calculation circuitry of 32 bit values is realized the synchronization of signal transmissions of 32 signal wirings. Disorder of signal waveform disturbs synchronization and transmission fail and error occur in the processing. Renewable energy systems are used in the harsh environment, for example electromagnetic radiation of lightning affects power source voltages fluctuation in FPGA [31]. Therefore, various timing margins are required in the internal circuitry. When the margins are enough, the disturbance could not affect the calculation result. On the contrary, when the margins are not enough, they may cause calculation errors.

When it is assumed that the FPGA circuitries have same characteristics, e.g. timing margin and wiring routes, they involve same errors caused from common environmental stresses. Therefore, the redundant systems cannot detect errors since common cause failures result same calculation outputs. On the contrary, when FPGA circuitries are different structures, it is expected the calculation results affected from the common cause failures are different each other under the same environmental stresses. Therefore, it is necessary to design the redundant control system with different FPFA circuitries under the consideration of common cause failure. It is also required to define the MTBF of redundant system which considers common cause failures.

Figure 4 shows a Markov model of self-repairing redundant system with common cause failure.



λ_{sub_sys} : The failure rate of a sub-system (1/hr)
μ_{sub_sys} : Repairer Rate of sub-system (1/hr)
β: Common cause failure fraction $(1 < \beta < 0)$
$P_0(t)$: Probability of both sub-system is in normal
$P_1(t)$: Probability of 1 sub-system fail
$P_2(t)$: Probability of both sub-system fail

Fig.4. Markov model of duplex system with common cause failure.

In Fig. 4, β factor is the common cause failure fraction $(1 < \beta < 0)$ of sub-systems. This Markov Model provides the following MTBF definition (see Appendix in detail);

$$\text{MTBF} = \frac{1}{\beta\times\lambda_{sub\_sys}} \quad (2)$$

where λ_{sub_sys} is the failure rate of a sub-system (1/hr).

Functional Safety Standard IEC-61508 specifies β in the part-6-Annex D [22]. The values of β ranges from 0.005 (0.5%) to 0.05(5%) in general. When λ_{sub_sys} of sub-systems in infrastructures is within 10^{-4} and β is 0.01, MTBF of one redundant system with common cause failures remains within 10^6 hours (about 100 years). In general, the renewable energy plant like a wind turbine consists of from 10 to 100 redundant controller systems. For example, when the energy plant system consists of 20 controllers, the MTBF of the whole plant becomes about 10^4 hours (about 5 years). This MTBF is insufficient for renewable energy plants which are installed in inconvenient places to maintain. In order to design reliable control systems by redundant FPGAs, the β value needs to be reduced.

To reduce the β value and realize the diversity of redundant system, one possible way is to combine the different FPGA circuitries. This combination of sub-systems with different-circuitry-FPGAs is named as diversity pair in this paper. In the following, the reliable control system by the diversity pair is discussed and evaluated.

3. Realization of Diversity

In general FPGA circuit design, first, HDL description is synthesized and translated in to logical netlist. Then, the FPGA configuration data is generated from the netlist by allocating physical gates resources for FPGA circuitries. The second design step is technology mapping. To realize the diversity of FPGA circuitry from common algorithms and common codes, the technology mapping is focused. FPGA compilers produce a huge number of circuit patterns, and select an optimal one by evaluating various parameters, such as wiring lengths and circuit performance. Many different implementation patterns are available as diversity, for one logic circuitry. The combination of the various implementation leads to huge diversity. This is advantageous in configuring redundant systems. Resource allocation in FPGA design can be controlled with compiler software. Figure 5 shows that different FPGA configuration data can be generated from the same HDL description by taking different resource allocation.

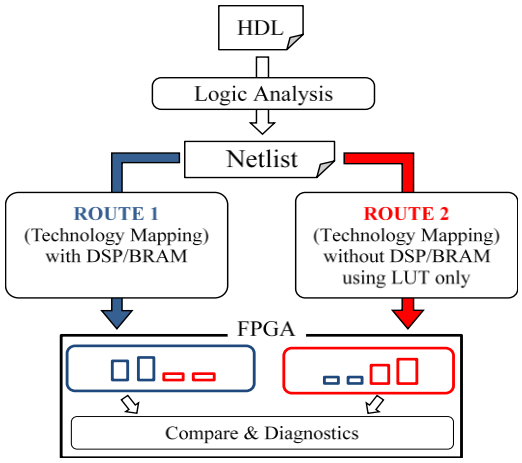


Fig.5. Image of DTM.

DSP is one of FPGA internal resources. It is special logic block for arithmetic, such as multiplication. BRAM is also internal resource of FPGA, functioning as memories. LUT, a resource of FPGA, is small memory usually used for configuring combinational circuit. LUT can also be utilized as small memory. Functionality of DPS and BRAM can be realized only with LUTs. For example, in Xilinx ISE FPGA design tool, resource allocation can be designated by directives. The following description is an example.

(*use_dsp48 = "no"*)

With this description, any DSP resources are not allocated, and only LUTs run calculations in the circuitries. This sort of resource allocation restriction in FPGA creates diversity, without changing HDL source code. Table 1 shows results of technology mapping of a multiplier on a Xilinx Kintex 7 FPGA. The results show that different implementation of the multiplier with different resource utilization were generated from the same HDL code.

Table 1. Comparison of Physical Parameters of DTM.

PHYSICAL PARAMETER OF FPGA	MULTIPLICATION (MUL)	
	ROUTE 1 (DSP)	ROUTE 2 (LUT)
Slice Logic Utilization		
Number of Slice Registers	0	0
Number used as Flip Flops	0	0
Number of Slice LUTs	38	1203
Number used as logic	38	1199
Number using O6 output only	38	590
Number using O5 output only	0	51
Number using O5 and O6	0	558
Number used exclusively as route-thrus	0	4
Number with same-slice carry load	0	4
Slice Logic Distribution		
Number of occupied Slices	24	316
Number of LUT Flip Flop pairs used	38	1203
Number with an unused Flip Flop	38	1203
Number with an unused LUT	0	0
Number of fully used LUT-FF pairs	0	0
Specific Feature Utilization		
Number of DSP48E1s	4	0
Average Fanout of Non-Clock Nets	1.61	2.68

Since FPGA circuitries generated in this way have different characteristics of resource usage, wiring patterns of them are also different. Thus, common cause failures are overcome by this diverse design methodology. We call this methodology as Diversity Technology Mapping (DTM). Another advantage of DTM is based on "Proven-In-Use", verified with sufficient records of utilization. It is very important concept for practical renewable energy plants [32].

4. Experiment and Evaluation

4.1. Simulation of Common Cause Failures

We explain a method of environmental stresses simulations and evaluate effect of DTM. To simulate common cause failure, we focus critical paths in FPGA. The critical path means the wiring path which has the smallest timing margin. It is considered that power supply drop results degradation of signal waveform in FPGA, reduces signal transmission efficiency, and causes delay of signal transmissions. The transmission delay suppresses circuit operational timing. The circuitries cannot complete signal transmissions within setting time windows for taking actions, resulting in a timing error. Effects of physical degradation and

electric field on FPGA also affect the signal transmission timing and cause timing errors. Overclocking can emulate those timing errors by changing the clock frequency of the circuit.

4.2. Test Environment

The target device for the evaluation is FPGA device, XC7K325-2 of Xilinx (kintex-7). Development software tool is Xilinx ISE 14.7. The four test cases shown Table 2 are evaluated, changing the clock frequency as shown in Table 2. Timing simulation is performed with random number inputs by 10,000 times for each clock frequency. Then, error rates and effect of DTM are evaluated.

4.3. Test Cases and Results

Simulation results are evaluated in terms of the following characteristics;

a) Error rate

b) Error detection rate

c) Error detection capability

Error rate is defined as a ratio of the error result to the correct one in 10000 trials. Error detection rate is defined as a ratio of the number when the diversity pair has different results to the number when one system of the diversity pair has an error result in 10000 trials.

Each test case is compared by the perspectives of the above characteristics as shown in Table 2. The FPGA clock frequency of each test case is executed from 120 MHz to 298 MHz. The data of following figures is focused on characteristic range for each test result because of the clarity as table 2.

Table 2. Test Case

Test Case No	Test Function	Clock Frequency (MHz)	No Divers Pair		No Divers Pair		Divers Pair (DTM)		Perspective		
			Mark	Route1/Route2	Mark	Route1/Route2	Mark	Route1/Route2	a	b	c
									Fig	Fig	Fig
1	Multiple	160~258	◆	DSP/DSP	■	LUT/LUT	●	DSP/LUT	6	10	14
2	PLI*	180~248	◆	BRAM/BRAM	■	LUT/LUT	●	BRAM/LUT	7	11	15
3	Cube	80~298	◆	DSP/DSP	■	LUT/LUT	●	DSP/LUT	8	12	16
4	MAC**	120~298	◆	DSP/DSP	■	LUT/LUT	●	DSP/LUT	9	13	17

*PLI : Piece-wide Liner Interpolation
**MAC: Multiply and Accumulate

Figures 6 through 9 show graph summaries of test results evaluated by the error rate. Error rates of circuitries with DSP or BRAM sharply rises at certain specific frequencies, and error rates for LUT based circuitries gradually rises along with clock frequency. These results are explained as following: when specified function blocks consist of DSP and BRAM, their signal propagation delays do not depend on input data values very much. On the other hand, the critical path of LUT-based circuits changes depending on input values. The difference of error curves reflects these mechanisms in FPGA circuits.

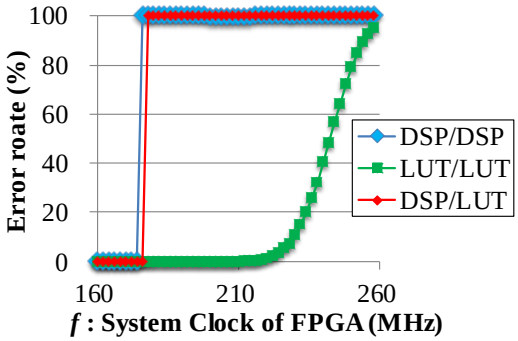


Fig.6. Error Rate of Test Case No. 1.

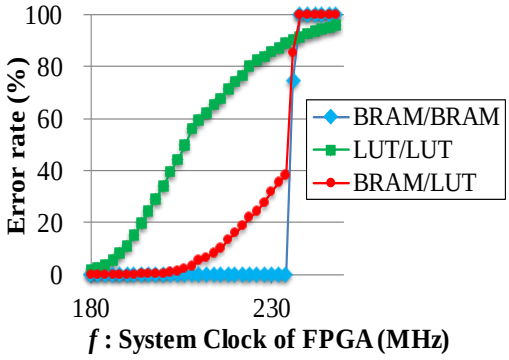


Fig.7. Error Rate of Test Case No. 2.

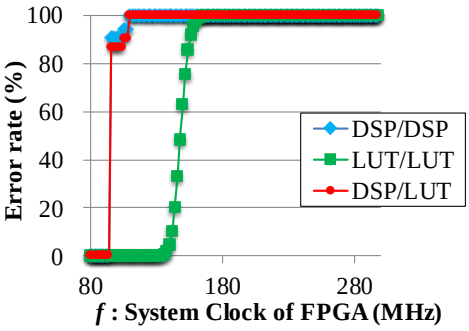


Fig.8. Error Rate of Test Case No. 3.

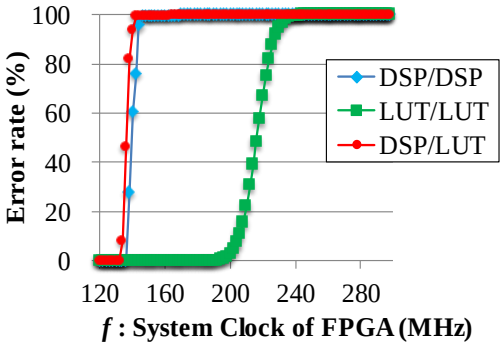


Fig.9. Error Rate of Test Case No. 4.

Figures 10 through 13 show the graph summaries of test results evaluated by the error detection rate. For DSP-only designs and BRAM-only designs, the error detection rate is zero for many frequency setups, since the pair produces the completely same error output values. This means that the redundant design does not contribute to the error detection.

For LUT-only designs, better error detection rates are achieved since they have different propagation delays depending on input data values. For DTM designs, much better error detection rates are achieved compared to other approaches, due to the diversity by the technology mapping.

From Fig. 10, it is seen that the result of DSP/DSP pair is almost same in case of the simple calculation which uses a few DSP resource. From Fig. 11, the error detection rate of BRAM/BRAM pair is constant 0 % to 234 MHz because that there is no error in the range.

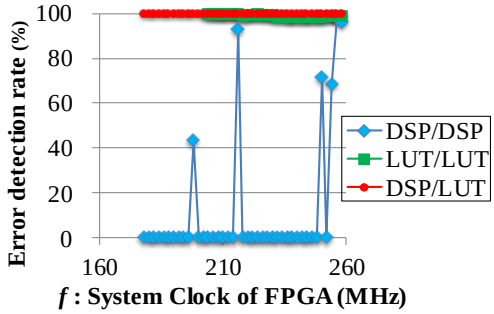


Fig.10. Error Detection Rate of Test Case No.1.

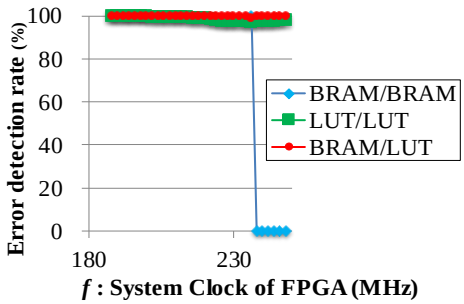


Fig.11. Error Detection Rate of Test Case No.2.

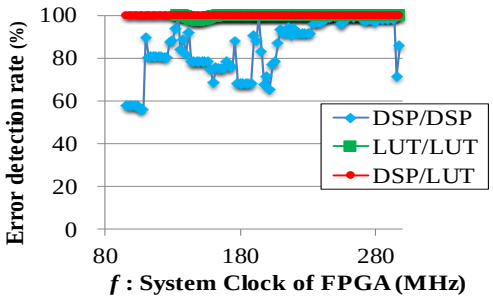


Fig.12. Error Detection Rate of Test Case No.3.

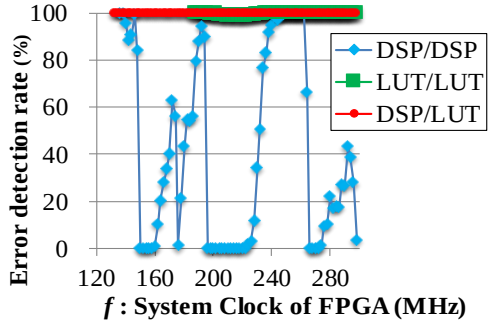


Fig.13. Error Detection Rate of Test Case No.4.

Only in 236 MHz, the discrepancies appear. But there is no discrepancy over 238 MHz. This causes from the characteristic of the RAM unit. From Fig. 12 and13, it is seen that the result of DSP/DSP pair has some discrepancies in case of the complex calculation which use several DSP resources. It is considered that this effect causes from the diversity effect of the wiring paths among the DSP units.

Figures 14 through 17 show graph summaries of test results evaluated by the error detection capability.

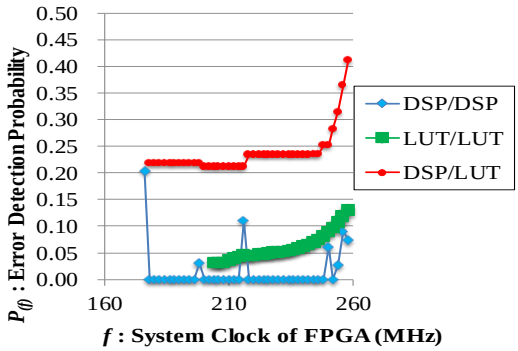


Fig.14. Error detection capability (Test Case No.1).

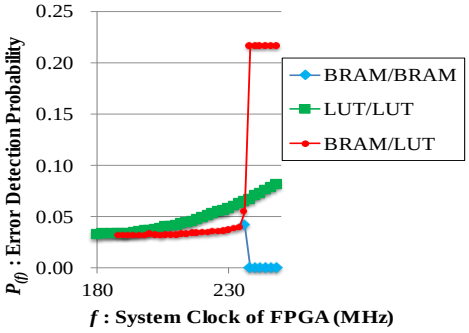


Fig.15. Error detection capability (Test Case No.2).

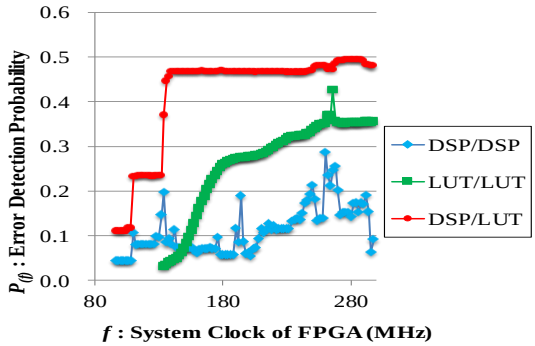


Fig.16. Error detection capability (Test Case No.3).

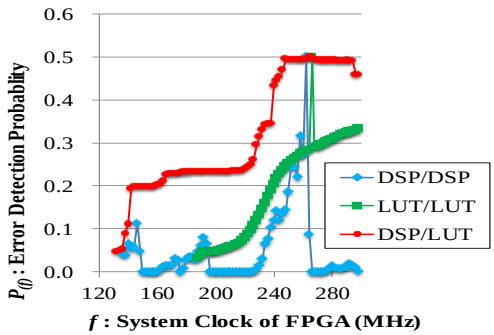


Fig.17. Error detection capability (Test Case No.4).

In these figures, the error detection capability $P_{(f)}$ is defined as Eq. (3);

$$P_{(f)} = \frac{\sum_{i=1}^{10^4} E(i,f)}{32 \times N(f)} \quad (3)$$

where f is the clock frequency, $E_{(i,f)}$ is the number of inconsistent bits in the i-th time test at frequency f, and $N_{(f)}$ is the number of errors occurred at frequency f. The probability means the number which is normalized by the length of data, that is 32 bits. $P_{(f)}$ = 0 means both 32-bit values are the completely same, and $P_{(f)}$ = 1 means every bit is different. $P_{(f)}$ can be considered as an index of detection capability of errors at frequency f. $P_{(f)}$ = 0 indicates that the errors cannot be detected even though they occur. Therefore, $P_{(f)}$ can also be considered as the error detection probability.

From Fig. 14 through 17, it is seen that the error detection probability of the diverse pair is higher than that of LUT/LUT pair, although the error detection rates of LUT/LUT pair are as same as the diverse pair. The different of the error detection probability between the diverse pair and the non-diverse pair is not so large. In following section, it is discussed that how the difference of the error detection probability of single function effects to the total control logic calculation.

4.4. Relation beta factor and DTM

The influence of diversity of functions to the entire control system is discussed based on the relation between the β factor and the proposed DTM. The control process can be described in the combination of the functions. One of the major description style is FBD (Function Block Diagram) language [7][33]. This paper focuses on control systems described by the FBD language. It is noted that the discussion here can hold other model based development languages such as MATLAB.

Figure 18 shows an example of the relation between the function block diagram and DTM. In this figure, it also shows the relation between the error detection probability and the miss-detection probability in the entire system.

When the control logic process consists of n function blocks, P_k means the error detection probability of the function block whose the calculation order number in the logic control process is k. P_k can be considered as the average probability of $P_{(f)}$ of the k-th function block in the previous section. Thus, $(1 - P_k)$ is the probability of the undetected probability when the result is identical although either controller has errors. $\prod_{k=1}^{n}(1 - P_k)$ means the probability that all calculation results of the function blocks between the redundant pair has no discrepancy in the entire process when the system contains some error. This probability can be considered as the equivalent value to β factor from Sec. 2.2.

$$\beta = \prod_{k=1}^{n}(1 - P_{k)} \quad (4)$$

P_k is different every kind of function blocks. In this discussion, it is supposed that variances of P_ks are close each other. $\bar{P}$ is defined as follows,

$$\bar{P} = \frac{1}{n}\sum_{k=1}^{n} P_k. \quad (5)$$

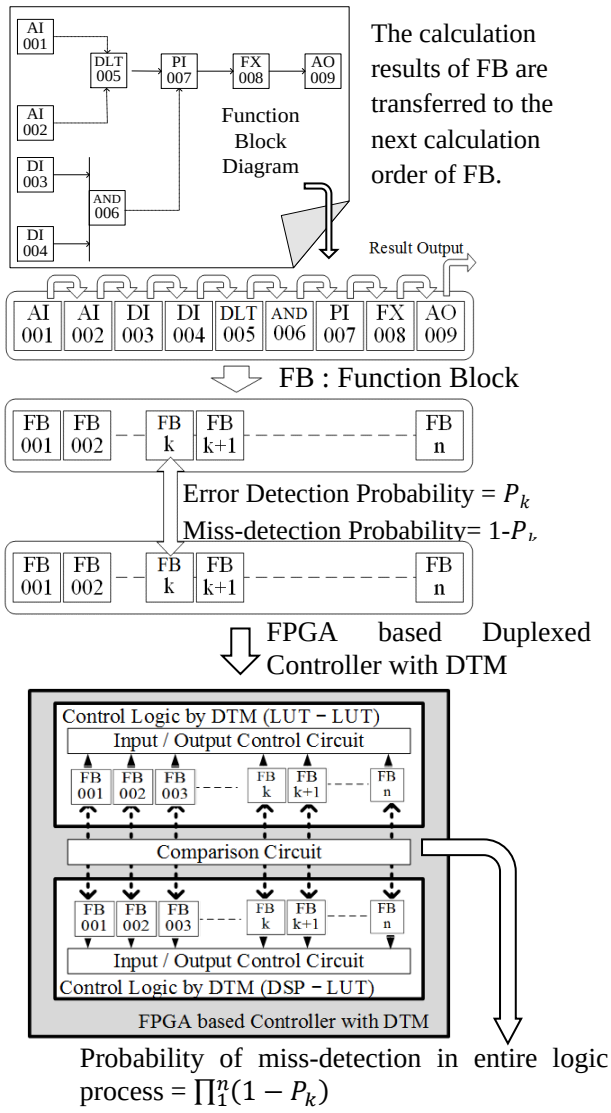


Fig.18. FBD based controller and DTM.

Then β factor is considered as follows,

$$\beta \approx (1 - \bar{P})^n \quad (6)$$

Theoretically β includes the error probability of the comparison circuit. Since the system has n comparison circuits, the probability that all comparison circuit makes error at same time is so small that it may be negligible.

Figure 19 shows the diversity effect to β and n. Comparison data is from the Table2, test case 1; Function is "Multiple", Pairs are "DSP/LUT(Red)" and "LUT/LUT(Green)". The sample data is chosen from 210 MHz to 258 MHz, and $\bar{P}$ is the average error detection probability $P_{(f)}$ of the sampling data. Since the difference of the error detection rate $\bar{P}$ between "LUT-LUT" and "DSP-LUT" is small, β factors are not so different each other when n is small, e.g. n=1, or n=5. Since β factors of "DSP-LUT" considerably decreases with increasing n, e.g. n=10, or n=20, The difference of β factors between "LUT-LUT" and "DSP-LUT" becomes large. The difference of β is more than 100 times larger, when n = 20.

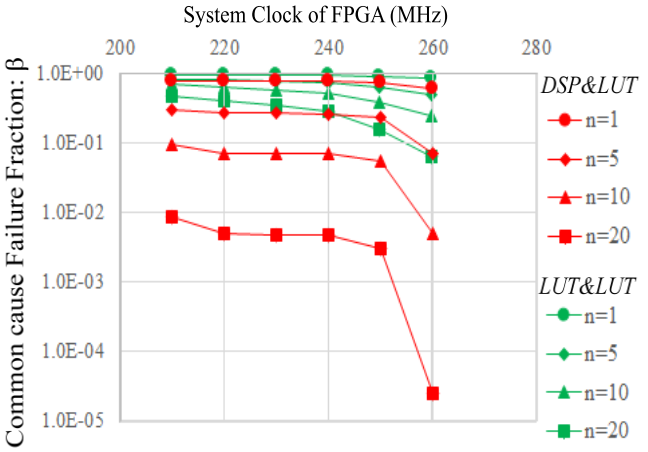


Fig.19. Diversity Effects, β versus Frequency and *n*.

Figure 20 shows the diversity effect against MTBF with β factors and the sub-system failure rate λ_{sub_sys}. MTBF = $\frac{1}{\beta \times \lambda_{sub\_sys}}$ from Eq. (2). And a year is used as the unit of MTBF. The sample test case is same as above. The failure rate of the sub-system is applied in case of 10^{-4}/hr,10^{-5}/hr and 10^{-6}/hr. In spite of the sub-system failure rate, it is confirmed that the MTBF improves more than 100 times by the effect of the decreasing common cause failure fraction β.

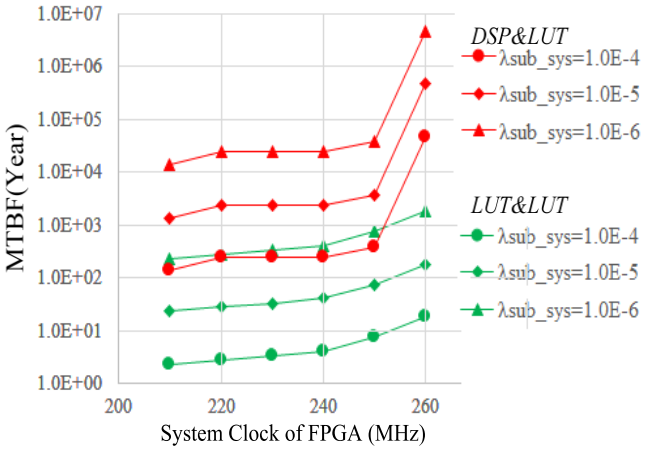


Fig.20. Diversity Effects, MTBF versus Frequency and Sub-system Failure Rate.

In addition, the industrial control system requires evaluations on basis of the functional safety standards [20]. The functional safety standard, IEC-61508, defines *PFD* (probability of failure on demand) of redundant systems as follows (refer to [20] IEC-61508 Part-6 Annex B B.3.2.2. 1oo2).

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \quad (7)$$

Table 3 shows meanings of coefficients and factors in Eq. (7) [20].

Table 3. Abbreviations of formula (7)

PFD_G	Average frequency of dangerous failure of the duplex system tests
λ_{DD}	Dangerous failure which is detected by the diagnostic
λ_{DU}	Dangerous failure which is not detected by the diagnostic
β_D	Rate of common cause failure which is detected by the diagnostic
β	Rate of common cause failure which is not detected by the diagnostic
t_{CE}	Channel equivalent mean down time
t_{GE}	Total equivalent mean down time
T_1	Proof time interval
$MTTR$	Mean Time To Repair
MRT	Mean Repair Time

In Eq. (7), β and β_D factors, common cause failure factor, determine PFD values, because the first term of the equation, the PFD value of redundant part, is so small and thus it is negligible. The standard defines the safety integrity levels (SIL). Table 4 shows definition of SIL in the standard. From the previous discussion of fig.19, β factors are improved and they range from 10 to 100 when *n*=10 and *n*=20. It means that increasing of the function blocks brings the low PFD value. Therefore, it is confirmed that this approach improves SIL of the functional safety.

Table 4. IEC-61508 Part1 7.6.2.9

Safety Integrity Level (SIL)	Average Probability of a Dangerous Failure on Demand of the Safety Function (PFDavg)
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 $<10^{-1}$

5. Conclusion

This paper presents a new approach, named DTM, which realizes diversification to the redundant FPGA circuitry although their algorithm, code and hardware conditions are remained same. DTM is the methodology which generates the diverse circuitries by the intentional FPGA resource distribution. The diverse FPGA circuitries generated by DTM are evaluated and it is confirmed that the diverse FPGA circuitries detect errors efficiently by the discrepancies of calculation results when the hardware stress causes the calculation error. It is also revealed that the DTM improves the Safety Integrity Level (SIL) of Functional Safety.Since this methodology uses the "proven-in-use" software tool, it fits for the industrial equipment e.g. infrastructures very much. It is most suitable for renewable energy because of the high reliability, the maintenance-fee, low cost and low exhaust heat of FPGA.

Appendix

A) Derivation of MTBF of Redundant system without Common Cause Failures

Markov Model of Fig. 3 shows $P_0(t)$, time-function, of probability that both sub systems stay in normal conditions. $P_1(t)$ is probability that one of sub systems is in abnormal conditions. $P_2(t)$ is probability that both systems are in abnormal conditions. Transferring from $P_0(t)$ to $P_1(t)$ occurs by failure ratio λ_{sub_sys} of either one of sub systems, then total ratio is $2 \times \lambda_{sub\_sys}$. In reparable systems, $P_1(t)$ transfers back to $P_0(t)$ by repair ratio μ_{sub_sys} is always 1 in power plant systems due to restoration by the spare system. The relations of $P_0(t)$, $P_1(t)$ and $P_2(t)$ are described by λ_{sub_sys} and μ_{sub_sys} as follows;

$$\frac{\mathrm{d}}{\mathrm{dt}}P_0(t) = -2\lambda_{sub\_sys}P_0(t) + \mu_{sub\_sys}P_1(t) \quad \text{(A.1)}$$

$$\frac{\mathrm{d}}{\mathrm{dt}}P_1(t) = 2\lambda_{sub_{sys}}P_0(t) - \mu_{sub_{sys}}P_1(t) - \lambda_{sub\_sys}P_1(t) \quad \text{(A.2)}$$

$$\frac{\mathrm{d}}{\mathrm{dt}}P_2(t) = \lambda_{sub\_sys}P_1(t) \quad \text{(A.3)}$$

Sub-systems are in normal conditions at start-up and initial values are as below;

$$P_0(0) = 1,\ P_1(0) = P_2(0) = 0 \quad \text{(A.4)}$$

MTBF is defined as an integration of $R(t)$ over time which is the probability that the system is in operable condition. $R(t)$ is either $P_0(t)$ or $P_1(t)$. Thus, MTBF defines as following;

$$\text{MTBF} = \int_0^\infty R(t)\,dt = \int_0^\infty (P_0(t) + P_1(t))\,dt \quad \text{(A.5)}$$

Solving earlier formula with equations (A.1) to (A.5);

$$\text{MTBF} = \frac{\mu_{\text{sub\_system}} + 3\lambda_{sub\_sys}}{2 \times {\lambda_{sub\_sys}}^2} \quad \text{(A.6)}$$

Substitute μ into the above formula, as earlier said, $\mu_{sub\_system} = 1 \gg \lambda_{sub\_sys}$

$$\text{MTBF} = \frac{1}{2 \times {\lambda_{sub\_sys}}^2} \quad \text{(A.7)}$$

B) Derivation of MTBF of Redundant system with Common Cause Failures

In Markov Model shown in Fig. 4, $P_0(t)$ is probability that both systems stay in normal conditions. $P_1(t)$ is probability that one of sub systems is in abnormal conditions. $P_2(t)$ is probability that both systems are in abnormal condition. Sub-system failure ratio λ_{sub_sys} is divided into common cause failures and others.

$$\lambda_{sub\_sys} = \quad (1-\beta) \times \lambda_{sub\_sys} + \beta \times \lambda_{sub\_sys} \quad \text{(B.1)}$$

$\beta \times \lambda_{sub\_sys}$ leads directly $P_1(t)$ to $P_2(t)$. Transferring from $P_0(t)$ to $P_1(t)$ occurs by failure ratio $(1-\beta) \times \lambda_{sub\_sys}$ of either sub systems, and the total ratio is $2\times\ (1-\beta) \times \lambda_{sub\_sys}$. In reparable systems, $P_1(t)$ transfers back to $P_0(t)$ by repair ratio μ_{sub_sys} is always 1 in power plant systems due to restoration with spare system. The relations of $P_0(t)$, $P_1(t)$ and $P_2(t)$ are described by λ_{sub_sys} and μ_{sub_sys} as follows;

$$\frac{\mathrm{d}}{\mathrm{dt}}P_0(t) = -\left(2 \times (1-\beta)\lambda_{sub_{sys}} + \beta \times \lambda_{sub_{sys}}\right)P_0(t) + \mu_{sub\_sys}P_1(t) \quad \text{(B.2)}$$

$$\frac{\mathrm{d}}{\mathrm{dt}}P_1(t) = 2 \times (1-\beta)\lambda_{sub_{sys}}P_0(t) - \mu_{sub_{sys}}P_1(t) - (1-\beta)\lambda_{sub\_sys}P_1(t) \quad \text{(B.3)}$$

$$\frac{\mathrm{d}}{\mathrm{dt}}P_2(t) = \beta \times \lambda_{sub\_sys}P_0(t) + (1-\beta)\lambda_{sub\_sys}P_1(t) \quad \text{(B.4)}$$

$$P_0(0) = 1,\quad P_1(0) = P_2(0) = 0 \quad \text{(B.5)}$$

Calculating MTBF with above formulas;

$$\text{MTBF} = \int_0^\infty R(t)\,dt = \int_0^\infty (\mathrm{P}_0(t) + P_1(t))\,dt \quad \text{(B.6)}$$

$$\text{MTBF} = \frac{\mu_{sub\_sys} + 3(1-\beta)\lambda_{sub\_sys}}{2(1-\beta)^2{\lambda_{sub\_sys}}^2 + \mu_{sub\_sys}\beta\lambda_{sub\_sys} + \beta{\lambda_{sub\_sys}}^2} \quad \text{(B.7)}$$

Substitute μ into the above formula, as earlier said, $\mu_{sub\_sys} = 1 \gg \lambda_{sub\_sys}$

$$\text{MTBF} \approx \frac{1}{\beta \times \lambda_{sub\_sys}} \quad \text{(B.8)}$$

References

[1] Y. Si, H. R. Karimi, H. Gao, "Parameter tuning for nacelle-based passive structural control of a spar-type floating wind turbine," in Proc. Industrial Electronics Society (IECON), pp. 7687-7691, Nov. 2013.

[2] N. Luo, Y. Vidal, L. Acho, Wind turbine control and monitoring, Springer International, 2014.

[3] M. K. Paul, B. Hamane, M. L. Doumbia, A. Cheriti, "Pitch control of a wind energy conversion system based on permanent magnet synchronous generator (PMSG)," in Proc. International Conference on Ecological Vehicles and Renewable Energies (EVER), pp. 1-7, Mar. 2015.

[4] I. Moussa, A. Bouallegue, A. Khedher, "3 kW Wind Turbine Emulator Implementation on FPGA Using Matlab/Simulink," in Proc. International Journal of Renewable Energy Research (IJRER), Vol.5, No.4, pp.1154-1163, 2015.

[5] D. Patterson, J. L. Hennessy, Computer Organization and Design, 5th Edition, Elsevier, Morgan Kaufmann, 2013.

[6] J. Cownie, "Multicore: the software view," in Proc. 12th EMEA ACADEMIC FORUM, Intel Corporation, 2007.

[7] IEC, "61131-1 Programmable controllers - Part 3: Programming languages Ed.3," Feb. 2013.

[8] K. H. John, M. Tiegelkamp, "Programming industrial automation systems," Springer International, 2001.

[9] H. Kim, A. K. Lu, R. Rajkumar, "A coordinated approach for practical OS-level cache management in multi-core real-time systems," in Proc. Euromicro Conference on Real-Time Systems, pp. 80-89, Jul. 2013.

[10] K. Gilles, S. Groesbrink, D. Baldin, T. Kerstan, "Proteus hypervisor: full virtualization and paravirtualization for multi-core embedded systems, embedded systems: design, analysis and verification," in Proc. IFIP International Embedded Systems Symposium (IESS), pp. 293-305, Jun. 2013.

[11] C. Wang, W. Li, J. Belanger, "Real-time and faster-than-real-time simulation of Modular Multilevel Converters using standard multi-core CPU and FPGA chips," in Proc. Industrial Electronics Society (IECON), pp. 5405-5411, Nov.2013.

[12] Y. Y. Tzou, T. S. Kuo, "Design and implementation of all FPGA-based motor control IC for permanent magnet AC servo motors," in Proc. International Conference on Industrial Electronics, Control and Instrumentation (IECON), vol.2, pp. 943-947, Nov. 1997.

[13] J. T. Welch, J. Carletta, "A direct mapping FPGA architecture for industrial process control application," in Proc. International Conference on Computer Design (ICCD), pp. 595-598, Sep. 2000.

[14] D.A. Lee, E.S. Kim, J. Yoo, J.S. Lee, J. G. Choi, "FBD to Verilog 2.0: an automatic translation of FBD into Verilog to develop FPGA," in Proc. International Conference on Information Science and Application (ICISA), pp. 1-4, May 2014.

[15] M. Kocur, S. Kozak, B. Dvorscak, "Design and implementation of FPGA - digital based PID controller," in Proc. International Carpathian Control Conference (ICCCC), pp. 233-236, May 2014.

[16] J. Khalifat, A. Ebrahim, A. Adetomi, T. Arslan, "A dynamic partial reconfiguration design for camera systems," in Proc. Adaptive Hardware and Systems (AHS), pp. 1-7, Jun. 2015.

[17] E.Monmasson, M.N.Cirstea, "FPGA design methodology for industrial control systems-a review," IEEE Transactions on Industrial Electronics, vol. 54, no. 4, pp. 1824-1842, Aug. 2007.

[18] G.Singh, S.S.Gill, "Design and Implementation of process controller for direct digital control on FPGA," in Proc. International Conference on Machine Intelligence and Research Advancement (ICMIRA), pp. 326-330, Dec. 2013.

[19] S.W.A.Hashmi, M.Rehan, M.Aamir, H.Kumar,F.Liaquat, "Distributed process monitoring and control using FPGA," in Proc. International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics System (VITAE), pp. 1-5, May 2014.

[20] A. M. Colak, Y. Shibata, F. Kurokawa, "FPGA implementation of the automatic multiscale based peak detection for real-time signal analysis on renewable energy systems," in Proc. International Conference on Renewable Energy Reserch and Applications (ICRERA), pp. 379 – 384, Nov. 2016.

[21] E. Irmak, I. Colak, H. I. Bulbul, N. Guler, A. Calpbinici, "FPGA based parallel connection system of separate voltage sources," in Proc. International Conference on Renewable Energy Reserch and Applications (ICRERA), pp. 1-3, Nov. 2012.

[22] IEC, "Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC-61508-Part1-7 ed2.0," Apr. 2010.

[23] A. Hayek, M AI-Bokhaiti and J. Borcsok, "Design and implementation of an FPGA-based 1004-architecture for safety-related system-on-chips," in Proc. International Conference on Microelectronics (ICM), pp. 1-4, Dec. 2013.

[24] R. Noji, S. Fujie, Y. Yoshikawa, H. Ichihara and T. Inoue, "Reliability and performance analysis of FPGA-based fault tolerant system," in Proc. IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT), pp. 245-253, Oct. 2009.

[25] F. Kastensmidt and R. Reis, "Soft error rate and fault tolerance techniques for FPGAs," Circuit Design for Reliability, Springer, pp. 207-221, 2015.

[26] M. Radu, "Reliability and fault tolerance analysis of FPGA platforms," in Proc. IEEE Long Island Systems Applications and Technology Conference (LISAT), pp. 1-4, May 2014.

[27] W. Wei, Y. Jun and Z. Mei-jie, "The research of FPGA reliability based on redundancy methods," in Proc. International Conference on Computer Science and Network Technology (ICCSNT), pp. 1608-1611, Dec. 2011.

[28] R. A. Ashraf, O. Mouri, R. Jadaa, R. F. Demara, "Design-for-Diversity for Improved Fault-Tolerance of TMR Systems on FPGAs," in Proc. International Conference on Reconfigurable Computing and FPGAs, pp. 99-104, Nov. 2011.

[29] L. A. Tambara, F. L. Kastensmidt, J. R. Azambuja, E. Chielle, F. Almeida, G. Nazar, P. Rech, C. Frost, M. S. Lubaszewski, " Evaluating the effectiveness of a diversity TMR scheme under neutrons," in Proc. International Conference on Radiation and Its Effects on Components and Systems (RADECS), pp. 1-5, Sept. 2013.

[30] T. Lovric, "Systematic and design diversity - Software techniques for hardware fault detection," in LNCS 852, Springer, pp. 307-326, Oct. 1994.

[31] T. Shindo, "Lightning strike fault risk on wind power generation system," in Proc. International Symposium on Electromagnetic Compatibility (EMC), pp. 593-596, May 2014.

[32] IEC, "Safety instrumented systems for the process industry sector, IEC-61511- ed2.0," Feb. 2016.

[33] K. Morimoto, Y. Shibata, Y. Shirakura, H. Maruta, F. Kurokawa, M. Nobe, M. Tanaka, "A New FPGA Based Green Controller Using Modeling Language," in Proc. International Journal of Renewable Energy Research (IJRER), Vol.6, No.2, pp. 715-722, 2016.