The safety review and formal verification on FPGA

ZUO Jiaxu[1], YU Wenzhuo[2], LI Sen[1], ZENG Hai[3], and ZHANG Chunming[1]

1. Department of Nuclear and Radiation Safety Research, Nuclear and Radiation Safety Center MEP, Beijing, 100082, China (zuojiaxu@chinansc.cn, lisen@chinansc.cn, zcm1106@sohu.com)

2. Special Risk Insurance Division, PICC Property and Casualty Company Limited, Beijing, 100022, China (yuwenzhuo1989@163.com)

3. Engineering Center, State Nuclear Power Automation System Engineering Corp, Shanghai, 200233, China (zenghai@snpas.com.cn)

Abstract: The FPGA technology is researched and developed in the reactor protection system. The FPGA system is developed by the software tools, and applications in the hardware. The safety review points of FPGA from NRC are introduced and some key points of FPGA's safety are discussed. The verification and validation, quality assurance and software tools seem more important for FPGA development. There are some disadvantages in the simulations of FPGA and the formal verification could be the usefully supplement for those disadvantages. Base on the SVA method in model checking of formal verification, the overpower ΔT trip chips were verified. And some bugs in ALU multiply modular were checked out and updated. Base on the SVA method, the formal verification makes the design and verification to take attentions on the function definition.

Keyword: nuclear safety review; simulation verification; formal verification; field programmable gate array

1 Introduction

The instrument and control (I&C) system is one of the most important systems in nuclear power plant (NPP). With the technology developing, the I&C system have updated with the development. The digital instrumentation and control system which bases on the CPU is the mainstream in NPP. At present, the Field Programmable Gate Array (FPGA) as the latest technology is researched and developed in the reactor protection system in nuclear power reactor[1, 2]. Also its safety review and verification both are the challenge in NPP.

2 The FPGA system in NPP

Until now, there are two kinds of methods to make FPGA active in I&C system in NPP. One method is that the FPGA takes the place of existed system. Because the complexity, which is caused by the operating software and the redundant functions, is reduced by FPGA. Another method is that the system is designed by FPGA in the new reactors. And the complexity functions and multiplicity will be considered carefully. The applications or the platforms based on FPGA could be used.

The FPGA platforms and main FPGA applications in US existing reactor systems are list in the following tables.

Table 1 shows the FPGA-Based Platforms in US nuclear industry. There are three platforms are under review or approved by NRC. The NuPAC platform is jointly developed by Lockheed Martin Corporation and SNPAS of SNPTC for reactor power plant.

Table 2 shows the main FPGA applications in US existing reactor systems.

Table 1 FPGA-based platforms in US nuclear industry

FPGA Platform	Applicant	Status
ALS	Westinghouse WEC/CSI	Approved
NuPAC	SNPAS&Lockheed-Martin	Under Review
Toshiba FPGA	Toshiba	Under Review

Table 2 Main FPGA applications in US existing reactor systems

Reactor Systems	Status	Applications
Wolf Creek	Completed and in Operation	FPGA used in main steam and feedwater isolation system in by Westinghouse/CSI
Diablo Canyon	Under Review	Use of ALS FPGA for Replacement of Digital RPS and ESFAS

Received date: January 12, 2015
(Revised date: February 12, 2015)

The first one is from the Wolf Creek Generating Station. Their application of FPGA used in main stream and feedwater isolation system in by Westinghouse/CSI. This application is completed and under operation.

Another is from the Diablo Canyon Nuclear Power Generating Station. They want to use of ALS FPGA for replacement of digital RPS and ESFAS. This application is under review.

3 Review of FPGA in NPP

3.1 Regulations and standards for FPGA in NRC

So far, there is no specific regulatory guidance on FPGA. But the regulatory for I&C is useful for FPGA's review.

The Regulatory and standard for I&C in NRC could be divided into different levels. The first level is the law, and it is 10 CFR 50.55 a(h). And the second level is the regulatory, and includes the NUREG-0800, RG 1.152 (IEEE 7-4.3.2-2003), RG 1.168 to RG 1.173, and so on.

There are also some standards and technical reports which could be reference. They are including the IEC 62566, EPRI TR 1019181, EPRI TR 1022983, NASA-HDBK 8739.23, RTCA/DO-254, NUREG/CR-6303, NUREG/CR-7007 and so on.

3.2 Regulations and standards for FPGA in China

The regulations of FPGA in China are also used for the I&C systems. And there is no specific regulatory guidance on FPGA too. This is one of the most difficulties for FPGA review. The regulations in China are shown in Table 3. And the regulations and standards from NRC would be also referenced.

3.3 Some key points of FPGA from review

From NRC's review, there are some key points, which are taken care in NRC's review, on FPGA technical in NPP.

The qualification on the software tools of FPGA development. The FPGA system is developed by the software tools, and applications in the hardware. The verification and validation, development history and corrective action of the software tools will be more and more useful to proof the reliability of tools.

Development process of FPGA applications is software-intensive and uses complex software tools to design and verify the applications. So there require high skills, specialized expertise, and qualified staff which is a disadvantage for FPGA applications. Under the review, the qualification of the development teams was also care. The team member, development history, team organizational, management and activities have to be review and manage.

Table 3 The regulations in China

Regulations	
The Safety Regulations on Nuclear Power Plant Design	HAF 102-2004
The Protection System and Related Facilities of Nuclear Power Plants	HAD 102/10-1988
The Safety Related Instrumentation and Control System in Nuclear Power Plant"	HAD 102/14-1988
Software for Computer Based Systems Important to Safety in Nuclear Power Plant	HAD 102/16-2004
Regulations on Supervision and Control of Civil Nuclear Safety Equipment	HAF 601-2007
Nuclear power plants-instrumentation and control system important to safety-software aspects for computer-based system performing category A functions	NB/T 20054-2011
Applicable criteria for digital computers in safety systems of nuclear power plants"	GB/T 13629-2008

The FPGA system software tools could contain latent defects/faults, and errors may exist in system or functional requirements and development process. The enough combinatorial testing approach and high quality life-cycle process is implemented. The high level verification and validation and quality assurance of FPGA is required and more important among the development cycle.

Final products of FPGA-based applications are purely hardware with no run-time software, but

don't treat FPGA-based applications as hardware-based systems.

Also, NRC considered that the failure mode and effects analysis (FMEA) for design reliability analysis will be very useful, but it also a very difficult work.

4 The verification of FPGA

From the FPGA development steps, it is shown that the verification process is the more useful to ensure the correctness of FPGA design. In addition to board-level simulation, there are three kinds of simulations in the traditional development process. For FPGA, there are two main methods to verification which are the simulation and formal verification. Both methods have their advantages and disadvantages.

4.1 The simulation verification of FPGA

The simulation verification is the mainstream methods. The function and timing verification can be operated for the RTL-level, gate-level and behavioral-level.

The step and flow of simulation verification is shown in Fig. 1. The arrows show the steps of the simulation verification.

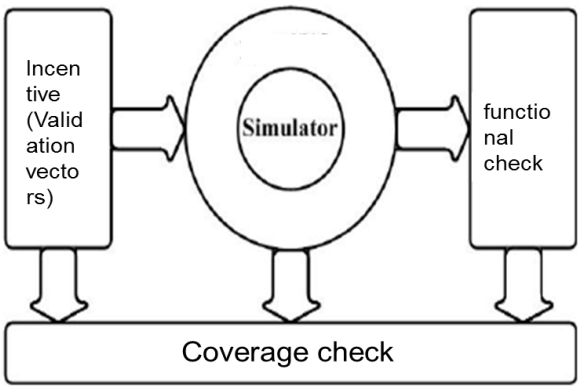

Fig.1 The flow of simulation verification.

The engineer must independently conceive the testbench to cover all of situations that may arise. And the accuracy of the design should be judged by the comparison the real output and theoretical output. And the verification could be finally completed by coverage rate analysis.

But it is difficult to fully cover in the simulation verification, and the testbench setting up and incentive conception are also complicated.

4.2 The formal verification of FPGA

The formal verification is to use mathematical methods (including the symbols and tools in the formal sense) to clearly describe the design requirements and the properties of the compiled system[3].

During the verification process, the symbols and tools would be used to test the requirements and the properties of the real design. The Fig, 2 shows the diagram of formal verification.

In General, there are three kinds of formal verification methods: theorem proving, model checking and equivalence[4].

With the advancement of technology, the theorem proving technology in formal verification has continued to be improved[5]. The temporal logic applied in reactive programs and the automatic verification of concurrent systems was solved[6]. But the state space explosion is appearance[7].

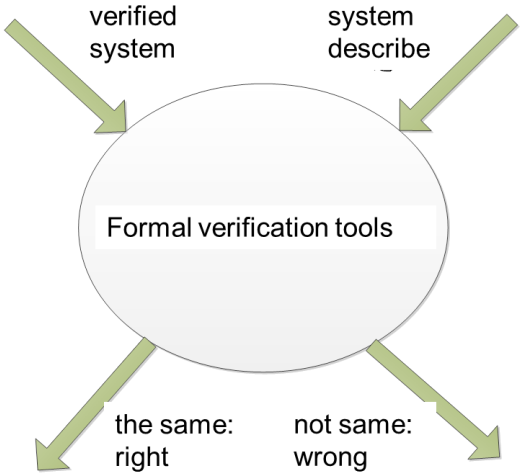

Fig.2 The diagram of formal verification.

But the formal verification is also the supplement of the simulation verification. The formal verification is with the following advantage: the high level of automation, the high completeness of verification, easy to adjust and debug. In the formal verification, the state will be exponential growth with the circuit scale. So the state explosion is the one of biggest disadvantage in it.

4.2.1 The theorem proving

The theorem proving defines a formal system, which is composed of axioms and inference rules. The mathematical descriptions of the circuit and the formal system are used to deduce and derive. The infinite state space could be deal with by the theorem proving. To prove the theorem proving is right, the needed formal description should be with the higher level than the RTL. And the fully process need the expert engineer to complete.

4.2.2 The model checking

The model checking based on finite state space. The nature and function of the system should be described by the mathematical logic. And then, the required function should be verified by the traverse all states of the system mode.

4.2.3 The equivalent

The equivalence is used to detect the consistent of design between the different steps in the development process. And the functional verification and validation of the RTL should have been correct[8, 9].

5 The formal verification of FPGA chip

5.1 The chip functions

The reactor protection system in the Protection and Safety Monitoring System (PMS) is one of the most important systems in the NPP. It works for the reactor safety and with the highest safety levels. In the NuPAC platform, this system is achieved by FPGA, and its simulation verification has been finished and correct[1, 2]. So the overpower ΔT trip chips will be used to formal verification. This chip will calculate the enter (cooling) and output (hot) temperature in primary loop to determine whether trip the reactor. Its signals logic is selecting 2 from 4. This FPGA chip includes the SRAM controller module and QDeltaT module. The QDeltaT module includes the ALU multiplier and six arbiter modules which the XFunction logic module is one of them. The function of XFunction is to calculate the function, and the results of that function will be as the input of next step. It also transmits the signal between the arbiters.

5.2 The verification method

Comparing the three methods of formal verification, the model checking method is the best path. The Fig. 3 shows the method selection process.

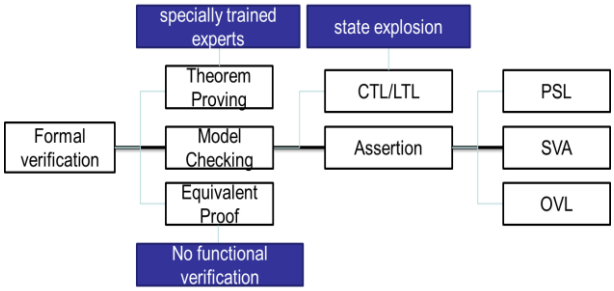

Fig.3 The formal verification method selection.

In this method, there are CTL/LTL (the Computation Tree Logic/the Linear Temporal Logic) and assertion. The state explosion is the most trouble in the CTL/LTL, so the assertion method is selected. The assertion is to describe how to perform a behavior in the function of the design. The assertions can be compiled into a Boolean expression structure, and it can be made the Boolean operations and step through to complete the checking[10]. The SVA, PSL and OVL in the assertion are compared too from different function. And it shows that the SVA method is the most easy to achieve[11].

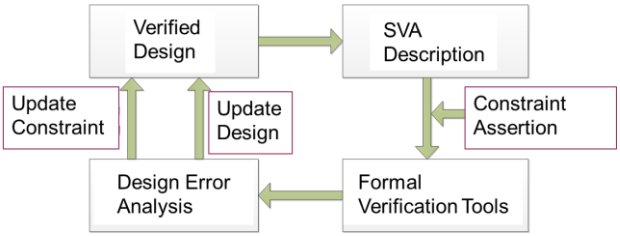

Fig.4 The SVA verification loops.

The SVA perfect describe timing-related program, with high level precision and simple. The Fig. 4 shows the SVA verification loops. There are five steps in the SVA, which are the environmental variable, the attribute assertions, the constraint assertions, connected with the design and the functional coverage.

We used the Questa Formal (Mentor Graphics) tools to finish the verification. In the assertion process, the Questa Formal will search all of the states, which are control by the environmental

variable and the attribute assertions, to verify the function and timing attributes of SVA.

5.3 The verification results

There are six attributes of SRAM. They are include the write-cycle control (tWC), the chip select time (tSCE), the write signal pulse width (tPWR), the interval of loading address to the end of write (tAW), the read cycles (tRC), the address access time (tAA). The SVA verification of six attributes shows all correct and full covered. Using model checking based on SVA, the RTL-level design like SRAM controller is verified. The results show that the simulation and formal verification are consistent.

The five main functions and several time series in ALU modular were verified. Total of ten SVA files and fifteen main attributes were used to assertion verification. The multiplication attributes is as an example to describe the test results. The multiplication attributes include the calculation function (Multiply_result_chk), the calculation recognition function (Multiply_in_chk), the computing cycle (Multiply_over_chk).

In the SVA verifications, the calculation function (Multiply_result_chk) validation result was "Fired", which means there are some wrong.

The counterexample waveforms of the ALU formal verification is shown in Fig. 5 and Fig. 6. The Fig. 5 shows the verification result of Multiply_result_chk is fired in two minutes. The Fig.6 shows the counterexample waveforms of the ALU formal verification.

Properties

	Name	Type	Check	Radius	Clocks
F	check0.a_Multiply_result_chk	sva	sva	28	sys_clock
P	check0.a_Multiply_in_chk	sva	sva		sys_clock
P	check0.a_Multiply_over_chk	sva	sva		sys_clock
C	check0.cov_Multiply_in_chk	sva	sva	2	sys_clock
C	check0.cov_Multiply_over_chk	sva	sva	27	sys_clock
C	check0.cov_Multiply_result_chk	sva	sva	27	sys_clock

Fig.5 The verification results of ALU multiplication function.

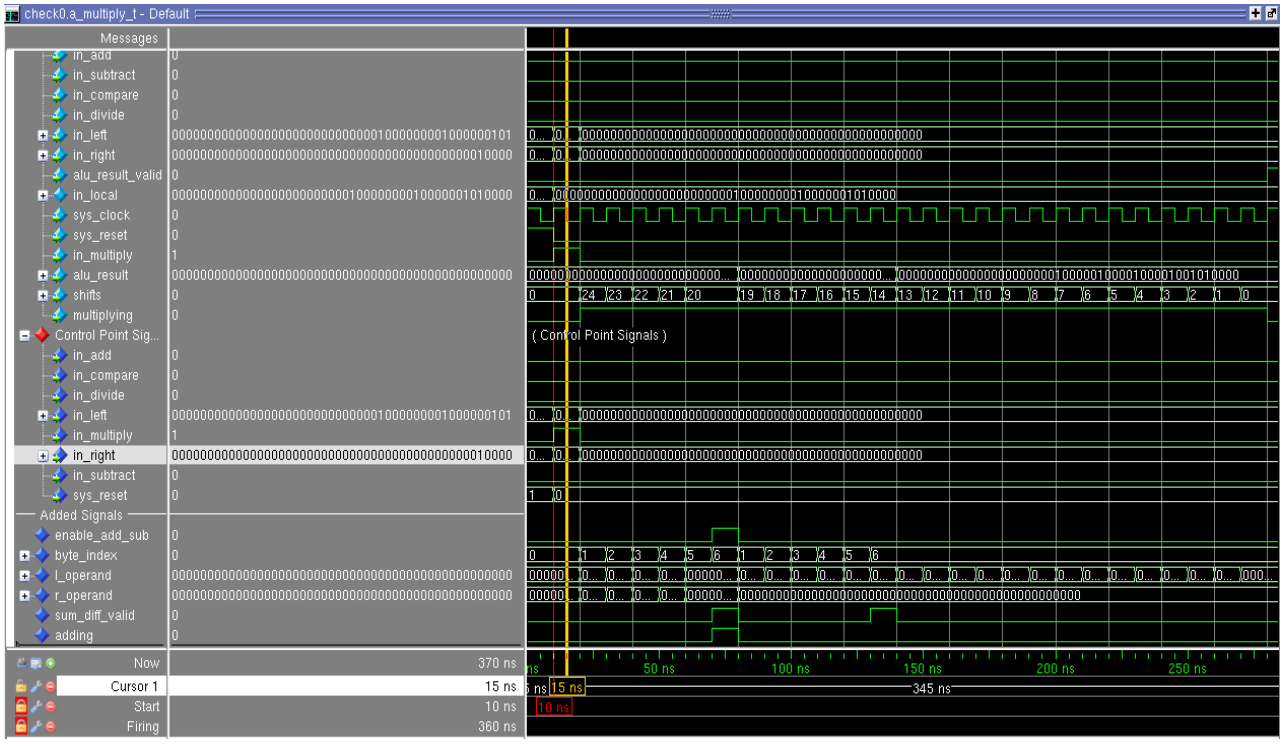

Fig.6 The counterexample waveforms of the ALU formal verification.

The mainly reasons are as following. In the source cord, the cycle start time of “byte_index” is not limited. If the “sum_diff_valid” is zero and the next moment the “enable_add_sub” is also zero, the “byte_index” will be counted when the “byte_index” is not equal to six.

The validation of the master device based on the XFunction as an example. The eight attributes of function modular in XFunction were used, and ten attributes of QDeltaT_top modular were used too. Those eighteen attributes were verified and all of them are correct and complete coverage. From the results, it could be shown that the simulation and formal are consistent in this part verification.

6 Summary

FPGA system is developed by the software tools, and applications in the hardware. How to deal with the reliability of FPGA in NPP is still a good question. Because of the high level design requirements for instrumentation and control system in NPP, the verification for FPGA is very important for the safety. The verification and validation, quality assurance and software tools are more important for FPGA development.

There are some disadvantages in the simulations of FPGA. From the example, it is shown that the formal verification could be the usefully supplement for those disadvantages. Base on the SVA method in model checking of formal verification, the overpower ΔT trip chips were verified. And some bugs in ALU multiply modular were checked out and updated. Base on the SVA method, the formal verification makes the design and verification to take attentions on the function definition. The formal verification can be used in the system and update the reliability of system.

Acknowledgement

Thanks for Reliability and verification and validation of nuclear safety I&C software Project (RAVONSICS) support and Thanks for Mr. Dai Ruidong and Ms. Xu Weiying’s useful discussions.

References

[1] ZENG Hai, SIEDLARCZYK I., and MAO Huan: Reactor Protection System of Nuclear Power Plant Based on NuPAC, Atomic Energy Science and Technology, 2014, 48(4): 692-697.

[2] ZENG Hai.: Key Characteristic Analysis of Reactor Protection System for Nuclear Power Plant Based on NuPAC, Atomic Energy Science and Technology, 2014, 48(3): 492-498.

[3] PERRY D., and FOSTER H.: Applied formal verification, McGraw-Hill, Inc., 2005.

[4] LU Yongjiang: Formal Verification Method of VLSI Research, Hangzhou: Zhejiang University, 2005.

[5] CHAN W., ANDERSON R J., and BEAME P., *et al.*: Model checking large software specifications, Software Engineering, IEEE Transactions on, 1998, 24(7): 498-520.

[6] GANAI M K., AZIZ A., and KUEHIMANN A.: Enhancing simulation with BDD and ATPG. Proceedings of 36th Design Automation Conference, 2001, 385-390p

[7] CHEN Li, and GAO Weiwei: The Formal Verification Method Review, VIEW, 2008, 7: 125.

[8] DATTW K., and DAS P P.: Assertion based verification using HDVL[C]//VLSI Design, 2004. Proceedings. 17th International Conference on. IEEE, 2004: 319-325.

[9] MA Tiemin: Front-end Design And Implementation of Equivalence Checking System of Verilog HDL, Changchun: Jilin University, 2012.

[10] VIJAYARAGHAVAN S., and RAMANATHAN M.: A practical guide for SystemVerilog assertions, Sspringer, 2006.

[11] DUDANI S., and HAVLICEK J.: The Power of Assertions in SystemVerilog, Springer, 2010.