Nuclear Engineering and Design 301 (2016) 311–319

Contents lists available at ScienceDirect

Nuclear Engineering and Design

journal homepage: www.elsevier.com/locate/nucengdes

Development, verification and validation of an FPGA-based core heat removal protection system for a PWR

Yichun Wu[a,*], Xuanxuan Shui[a], Yuanfeng Cai[a], Junyi Zhou[a], Zhiqiang Wu[b], Jianxiang Zheng[a]

[a] College of Energy, Xiamen University, Xiamen 361102, China
[b] State Key Laboratory of Reactor System Design Technology, Nuclear Power Institute of China, Chengdu 610041, China

HIGHLIGHTS

- An example on life cycle development process and V&V on FPGA-based I&C is presented.
- Software standards and guidelines are used in FPGA-based NPP I&C system logic V&V.
- Diversified FPGA design and verification languages and tools are utilized.
- An NPP operation principle simulator is used to simulate operation scenarios.

ARTICLE INFO

Article history:
Received 2 December 2015
Received in revised form 10 March 2016
Accepted 16 March 2016
Available online 30 March 2016

ABSTRACT

To reach high confidence and ensure reliability of nuclear FPGA-based safety system, life cycle processes of discipline specification and implementation of design as well as regulations verification and validation (V&V) are needed. A specific example on how to conduct life cycle development process and V&V on FPGA-based core heat removal (CHR) protection system for CPR1000 pressure water reactor (PWR) is presented in this paper. Using the existing standards and guidelines for life cycle development and V&V, a simplified FPGA-based CHR protection system for PWR has been designed, implemented, verified and validated. Diversified verification and simulation languages and tools are used by the independent design team and the V&V team. In the system acceptance testing V&V phase, a CPR1000 NPP operation principle simulator (OPS) model is utilized to simulate normal and abnormal operation scenarios, and provide input data to the under-test FPGA-based CHR protection system and a verified C code CHR function module. The evaluation results are applied to validate the under-test FPGA-based CHR protection system. The OPS model operation outputs also provide reasonable references for the tests. Using an OPS model in the system acceptance testing V&V is cost-effective and high-efficient. A dedicated OPS, as a commercial-off-the-shelf (COTS) item, would contribute as an important tool in the V&V process of NPP I&C systems, including FPGA-based and microprocessor-based systems.

1. Introduction

Field-programmable gate arrays (FPGAs) and similar programmable logic devices (PLDs) have gained increased attention worldwide for nuclear power plant (NPP) instrumentation and control (I&C) applications, including safety and non-safety systems (EPRI 1019181, 2009). As opposed to microprocessor based systems, FPGA/PLD-based systems can be made simpler and less reliant on complex software such as operating systems (EPRI 1022983, 2011). It results in lower complexity and simpler verification and validation (V&V) efforts (IAEA NP-T-3.17, 2016). FPGA can also enhance safety margins of the plant with potential possibility for power upgrading at normal operation (She and Jiang, 2011). Since the memory and logic in FPGAs are susceptible to single event upsets (SEUs), proper design techniques must be employed to ensure reliability (Wang et al., 2011).

Effective implementation of FPGA/PLD technology in NPP I&C systems is highly dependent on the successful development and use of regulations, regulatory guidance and standards. IEC 62566 (IEC 62566, 2012) is an international standard that provides

* Corresponding author. Tel.: +86 592 5952733.
E-mail addresses: ycwu@xmu.edu.cn (Y. Wu), 807001564@qq.com (X. Shui), 1056303902@qq.com (Y. Cai), 1032133755@qq.com (J. Zhou), npic_wu@126.com (Z. Wu), zwu@xmu.edu.cn (J. Zheng).

http://dx.doi.org/10.1016/j.nucengdes.2016.03.018
0029-5493/

guidance and requirements to achieve safety FPGA/PLD-based NPP I&C systems, complements IEC 60987 (IEC 60987, 2007) (at hardware level) and IEC 60880 (IEC 60880, 2006) (at software level). However, this standard has not been widely accepted by national regulatory bodies and does have limitations. Currently, most national regulators (such as the U. S. Nuclear Regulatory Commission (U.S. NRC)) apply existing regulations, guidance and standards for microprocessor-based systems to review, certify and license FPGA/PLD-based applications (NUREG/CR-7006, 2009). IAEA NP-T-1.13 report recommends that logic implemented on FPGA/PLD should be verified according to software V&V standards and guidelines (IAEA NP-T-1.13, 2015). However, most of those software standards and guidelines do not include FPGA/PLD specific attributes. Therefore, the purpose of this paper is to provide a specific example on how to conduct life cycle development process and V&V on FPGA-based CHR for pressure water reactor (PWR).

Chinese nuclear power industry is actively studying and developing FPGAs in their NPP I&C systems. For example China's State Nuclear Power Automation System Engineering Company and Lockheed Martin Global, Inc. have been cooperatively developing FPGA-based digital safety I&C platform for Chinese CAP1400 reactor design (LMGI, 2012). It is important for Chinese I&C vendors, licensees and the National Nuclear Safety Administration (NNSA) to agree on the regulations, guidance and standards that will be applied to the license of FPGA/PLD-based NPP I&C system.

V&V processes are performed in parallel with all life cycle stages, and provide an objective assessment of products and processes throughout the life cycle (IEEE 1012, 2012). It is one of the key issues for the application and license of FPGA/PLD-based safety I&C systems. In this paper, the development and V&V process of an FPGA-based core heat removal (CHR) protection system for CPR1000 PWR is detailed. CPR1000 is a three-cooling-loop 1000 MWe PWR, which is an updated version of Chinese Daya Bay nuclear reactor (Zhang et al., 2012). Due to the lack of commercial FPGA-based I&C platform, the CHR protection system is a simplified system. However, the development and V&V methods presented in the paper are generic and also suitable for commercial applications. The CHR system consists of three sub-functions: over temperature ΔT (OTΔT) reactor trip, over power ΔT (OPΔT) reactor trip and reactor trip on low primary coolant flow (LPCF). The NPP safety I&C system related IEEE standards are applied as the guiding documents in this project.

In the system acceptance testing V&V phase, an NPP operation principle simulator (OPS) model simulates CPR1000 PWR operation scenarios, including normal and abnormal operations, and provides inputs to the under V&V FPGA-based system. Based on the WSC's (Western Services Corporation) 3KEYMASTER simulation platform (WSC, 2010), the NPP OPS models a CPR1000 PWR NPP. It utilizes the light water reactor transient estimate code RELAP5 R/T (Idaho National Laboratory, 2012) to establish nuclear island models, uses the FlowBase tool to construct fluid network models and applies the Logic tools to simulate control systems. The major systems of the NPP primary and secondary loops are modeled. The OPS model is able to simulate the reactor core physics and the thermal hydraulic characteristics of various equipment and systems. With abundant graphics, instrument displays, alarm signals, etc., it vividly exhibits the basic principles of a CPR1000 NPP and its systems.

Lee et al. (2009) presented a NPP full-scope engineering simulator (FES) that is not only designed and used as the operators training platform, but also provided for V&V of the non-safety digital systems. The NPP FES was also proposed in the system assessment of an FPGA-based reactor protection system (RPS) (Lu et al., 2015a) and the evaluation of an FPGA-based fuzzy logic control of feed-water for ABWR NPP (Lu et al., 2015b). One major difference between the FES and the OPS is that the OPS has no real digital I&C systems and panels. Therefore, the cost of OPS is much lower than FES. The Ningde NPP FES has the same simulation model as the OPS model of this project has. Ningde NPP has four CPR1000 PWRs and located in Fujian province, China (Zeng et al., 2016).

The rest of the paper is organized as follows: Section 2 describes the FPGA-based CHR protection system for CPR1000 PWR, and Section 3 provides the life cycle of FPGA-based I&C. Section 4 details about the development and V&V of the FPGA-based CHR protection system, including the V&V system acceptance test platform development and test results analysis. Finally, the paper concludes in Section 5.

2. An FPGA-based core heat removal protection system for PWR

The reactor trip system (RTS) performs the reactor scram function, which is qualified as a Class 1E safety system. As a subsystem of the RTS, the CPR1000 CHR protection system provides the following reactor trip functions: OTΔT reactor trip, OPΔT reactor trip and reactor trip on LPCF.

The OTΔT trip protects the reactor core to against departure from nucleate boiling (DNB) for combinations of coolant temperature, power, pressure, and axial power deviation. Since DNB will reduce the heat transfer coefficient between the fuel rods and the reactor coolant, then result in the fuel cladding temperature increases. The purpose of OPΔT protection trip is to prevent the high power density of fuel rods, and the result of fuel rod cladding damage and fuel melt. In the event of low primary coolant flow, the reactor trip on LPCF protects against DNB.

In the RTS functions, the OTΔT and OPΔT trips are two relatively complex sub-functions and need floating point calculation and digital filters. While the LPCF trip is a typical logical function.

3. The life cycle process for FPGA-based I&C system

FPGA is a mix of software and hardware. As part of the life cycle methodologies, rigorous V&V approaches as defined in IEEE 1012-2012 are adopted in the FPGA software part of the development. The FPGA hardware development could follow IEC 60987 (IEC 60987, 2007; Allen et al., 2012). The development and V&V process of this project follows the life cycle process presented in Fig. 1. Initially, the stakeholder requirements are transformed into system requirements. Next, the system requirements are divided into software requirements and hardware requirements. Then the software and hardware are independently developed, including requirements analysis, architectural design, implementation and integration. In the system integration phase, the software items and hardware items are integrated into a completed system, which must satisfy the system design and the stakeholders' expectations. From this phase, the FPGA system is regarded as a pure hardware system. The system acceptance testing process assures that the system satisfies its acceptance criteria and enables the customer to determine whether or not to accept the integrated system product.

4. The FPGA-based CHR protection system development and V&V

IEC 61508-2010 (IEC 61508, 2010) defines four safety integrity levels (SIL) providing a relative indication for the criticality of a particular software component to an overall system. The SIL classification level defines the minimum tasks required for each V&V activity by IEEE 1012-2012 (IEEE 1012, 2012). The CPR1000 NPP CHR system provides safety critical protection function. Therefore, all software components for this project are assigned to have SIL4 value. Organizationally, independent V&V is needed. The V&V team not only reviews all of the test results provided by the design team,