ORNL/NRC/LTR-07/06

Survey of Field Programmable Gate Array Design Guides and Experience Relevant to Nuclear Power Plant Applications

July 2007

Prepared by
M. Bobrek, D. Bouldin, D. Holcomb, S. Killough, S. Smith, and C. Ward

NRC Manager: M. Waterman
ORNL Manager: R. Wood

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ORNL/NRC/LTR-07/06

Engineering Science and Technology Division

Survey of Field Programmable Gate Array Design Guides and Experience Relevant to Nuclear Power Plant Applications

M. Bobrek, D. Bouldin, D. Holcomb, S. Killough, S. Smith, and C. Ward

NRC Manager: M. Waterman
ORNL Manager: R. Wood

FPGA Design Guidelines

July 2007

Prepared for
U.S. Nuclear Regulatory Commission
under
DOE Interagency Agreement 1886-T241-06
NRC JCN No. N6351

Prepared by the
OAK RIDGE NATIONAL LABORATORY
P.O. Box 2008
Oak Ridge, Tennessee 38731-6285
managed by UT-Battelle, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

Page

LIST OF ACRONYMS

ASIC	application-specific integrated circuit
BIST	built-in self-test
BRAM	block random access memory
CPLD	complex programmable logic device
DCM	digital clock manager
ESA	European Space Agency
ESD	electrostatic discharge
ESF	engineering safety feature
FMEA	failure mode effects analysis
FPGA	field-programmable gate array
FTA	fault tree analysis
HDL	hardware description language
I&C	instrumentation and controls
I/O	input/output
IV&V	independent verification and validation
JTAG	joint test action group
LUT	lookup table
NASA	National Aeronautics and Space Administration
NRC	Nuclear Regulatory Commission
ORNL	Oak Ridge National Laboratory
PLD	programmable logic device
SEE	single-event effect
SEU	single-event upset
SRAM	static random access memory
TDDB	time-dependent dielectric breakdown
TID	total ionizing dose
TMR	triple-modular redundancy
UVA	University of Virginia
V&V	verification and validation

1 INTRODUCTION

Oak Ridge National Laboratory (ORNL) has been engaged by the U. S. Nuclear Regulatory Commission's (NRC) office of Nuclear Regulatory Res. to develop the technical basis for assessing field programmable gate array (FPGA) technology in safety-related systems within nuclear power plants. In particular, ORNL has investigated programmable digital logic technology and implementation practices to support development of review guidance. As part of this study, ORNL has surveyed information on the use of FPGA technology for high-assurance applications. This report presents the findings of these surveys, along with a summary of particularly relevant programmable logic device standards.

Information for this report was obtained through publicly available sources such as published papers and presentations. No proprietary information is represented.

1.1 BACKGROUND

An FPGA is a digital device containing programmable logic components and programmable interconnects. The logic components can be programmed to duplicate the functionality of basic logic gates such as AND[1], OR[2], XOR[3], NOT[4], or more complex combinational[5] functions such as decoders or simple math functions. Also, the programmable logic can include memory elements such as simple flip-flops[6] or more complete blocks of memories.

FPGAs emerged more then two decades ago as a normal process of constantly increasing integration level in digital electronics. They offered a significant improvement in the digital design by moving the logic block interconnects from the designer's responsibility to the specialized synthesis, place, route, and simulation tools. This simple paradigm enabled several major advantages of the FPGA-based design over the existing glue-logic design that was based on extensive board-level interconnects. First, FPGA design tools offer automatic detection and/or correction of many typical errors that were much more difficult to detect and correct in the old design environment. Second, moving the interconnects from the board level to the silicon level enables a huge reduction in size, power, and price of digital systems. Third, many of the tedious design steps that were prone to errors are now performed by the FPGA manufacturer so that the whole process can be standardized, tested, and constantly improved. Fourth, FPGA feature sizes are continually decreasing, allowing manufacturers to pack more logic into a single chip. FPGAs today use 65nm technology with close to 10 million basic logic gates in a single chip. Many of the mentioned advantages of the FPGA technology make it inherently more reliable and safe for use in critical applications. Obviously, the increased complexity requires special care when FPGAs are used in safety-critical systems.

In further detail, a hierarchy of programmable interconnects allows the logic blocks of an FPGA to be interconnected as needed by the system designer, somewhat like a one-chip programmable breadboard. The FPGA designer can program these logic blocks and interconnects after the chip manufacturing process (hence the term "field programmable"), so that the FPGA

[1] AND is a digital logic gate that only outputs a high (1) result when both inputs are high. Otherwise, the output is low (0).

[2] OR is a digital logic gate that outputs a high (1) result when either input is high. Otherwise, the output is low (0).

[3] XOR is a digital logic gate that outputs a high (1) result when only one input is high. Otherwise, the output is low (0).

[4] NOT is a digital logic gate that is essentially an inverter. If the input is low (0) then the output will be high (1) and vice versa.

[5] Combinational logic is logic whose output is a function of the present input.

[6] Flip-flops are electronic circuits with two stable states that are capable of serving as one bit of memory.

can perform whatever logical function is needed. Not all FPGAs are truly field reprogrammable. Vendors often sell less flexible versions of their FPGAs, which cannot be modified after the design is committed. For safety applications, this has the advantage of permanently committing the logical functions into an invariant form.

The FPGA design process begins with the designer creating a hardware description language (HDL)[7] or a schematic design of the desired logical functions. Common HDLs are VHDL[8] and Verilog[9]. Then, using an electronic design automation tool, a technology-mapped netlist[10] is generated. The netlist can then be fitted to the actual FPGA architecture using a process called place-and-route, usually performed by the FPGA company's proprietary place-and-route software. Different companies' place-and-route software packages are likely to implement the same logical functions in different physical layouts. The next step in a typical FPGA design process is for the designer to validate the place-and-route results via timing analysis and performance simulation. Once the design and validation process is complete, the binary file generated (also using the FPGA company's proprietary software) is used to (re)configure the FPGA.

In an attempt to reduce its complexity, the abstraction level of the HDL design can be raised. A number of FPGA design tools that use high-level languages such as System-C, LabVIEW, Matlab, SystemVerilog, SystemVHDL, and Handel-C have been recently developed. To further simplify the design of complex systems in FPGAs, libraries of predefined complex functions and circuits, with widely varying performances in speed, accuracy, reliability, etc., are commonly employed as a block to avoid having to recreate previously developed logic.

Generally, FPGAs can perform any arbitrary logic function for which they have been programmed, so they can be deployed in nuclear power plants in place of any logic function component such as trip logic units, engineering safety feature (ESF) actuation decision logic, or digital communication interface priority logic. Due to their technical capabilities, FPGAs are currently widely deployed for industrial applications requiring fixed or infrequently changing logical functions.

FPGAs constitute a broad technology class with differing implications for their application to safety systems based on the particular details of the implementation. In its simplest form, an FPGA could be restricted to implementing small logic blocks such as interdivisional voting. This type of implementation would likely lack any system memory (signal history), and therefore may be sufficient to be completely and deterministically analyzed and tested.

In a more advanced form, the FPGA could possess memory functions and a set of basic math functions. This type of FPGA would very likely be designed, validated, and tested using computer-based tool sets based on some form of formal verification. The logic implementing this type of FPGA would almost certainly be too complicated to be completely validated analytically, due to the extremely large number of possible logic states. Even more advanced logical functions can be implemented within FPGAs, including embedded microprocessors with their related peripheral components, enabling the creation of system-on-a-chip devices. These types of systems include both the digital logic and software designs, greatly increasing the overall complexity of the validation process.

[7] HDL describes the components operation, design, and organization.

[8] VHDL stands for **V**HSIC (Very High Speed Integrated Circuit) **H**ardware **D**escription **L**anguage and is the most common software for FPGA and ASIC designs.

[9] Verilog is another HDL for FPGAs and ASICs. Its syntax is similar to C programming language.

[10] A netlist describes the connections that need to be made for the design.

Even though the FPGA design involves hardware implementation of logical functions, the design process itself is highly software intensive. Hence, errors within the software design process can result in undesired behavior of logical functions implemented in hardware. In this case, the software validation process shifts from the application software to the certification of the FPGA design tools.

1.2 RESEARCH APPROACH

From a safety perspective, it is difficult to assess the correctness of FPGA devices without extensive documentation, tools, and review procedures. NUREG/CR-6463, “Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems,” provides guidance to NRC staff for auditing of safety system programs written in ten high-level languages. A uniform framework for the formulation and discussion of language-specific programming guidelines was employed. Comparable guidelines based on a similar framework are needed for FPGA-based systems. It is the objective of this project to develop the technical basis for these guidelines.

The first task in this research involves evaluation of regulatory experience gained by other countries and other agencies, and those captured in existing standards, to identify regulatory approaches that can be adopted by NRC. If existing regulations do not provide a sufficient regulatory basis for adopting relevant regulatory approaches that are uncovered, ORNL will identify the gaps. This report presents the findings of this research activity.

1.3 REPORT ORGANIZATION

This report contains summaries of documents discussing the use of FPGAs in safety-critical systems. The summaries are divided into two main sections: 1) Regulatory Approaches by Other Countries and Agencies, and 2) Existing Standards. The first section contains documents found with regulatory experience from Japan and France. The remaining section is composed of documents dealing with the aerospace industry, which includes those from the European Space Agency (ESA), the National Aeronautics and Space Administration (NASA) and general FPGA findings for space, the nuclear industry, and finally, the automotive industry. The final section includes the existing standards like Design Assurance Guidance for Airborne Electronic Hardware, DO-254[11].

2 FPGA-RELATED TECHNICAL STANDARDS/ PUBLISHED MATERIAL

Internet searches of technical standards related to FPGA design were performed. The main goal was to find FPGA design standards from other countries, industries, etc. to assess and possibly adopt as a basis for reviewing FPGA-based nuclear power applications. Although the searches did not turn up any standard dedicated to the use of FPGAs, a total of 85 documents were identified as relevant. The material was then examined more closely for topics relating to the following:

- Integrity of the FPGA programming process and methods of FPGA code and hardware verification and validation (V&V)

[11] DO-254 is a standard for complex electronic hardware created by the Radio Technical Commission for Aeronautics (RTCA), which develops standards for the Federal Aviation Administration (FAA).

- Single event effects (SEEs) and the techniques to reduce/eliminate their impact on the FPGA functionality
- Safe hardware design practices specific to FPGAs

Of the 85 documents, 21 were selected based on the above criteria for further review. The selected documents are listed below:

Regulatory Approaches by Other Countries and Agencies

- Transition and Current Status of NPP C&I System of BWRs in Japan
- PLD-Based Safety Critical Systems: An Introduction and Survey
- A Comparison of Radiation-Hard and Radiation-Tolerant FPGAs for Space Applications
- Formal Verification of Fault Tolerance in Safety-Critical Reconfigurable Modules
- Lessons Learned From FPGA Developments
- Application-Specific Integrated Circuit (ASIC) Design and Manufacturing Requirements
- Independent Verification and Validation: First Year Summary Report for the Programmable Logic Devices Research
- A Preliminary Practitioner's Guide to Defect Detection in VHDL Based Designs
- Architectural Principles for Safety-Critical Real-Time Applications
- Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants
- AP1000 Instrumentation and Controls
- Design, Test, and Certification Issues for Complex Integrated Circuits
- FPGA Space Qualification Presentation
- Suitability of Reprogrammable FPGAs in Space Applications
- VHDL Modeling Guidelines
- Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- Reliability Considerations for Automotive FPGAs
- Embedded Digital System Reliability & Safety Analyses (NUREG/GR-0020)

Existing Standards

- Design Assurance Guidance for Airborne Electronic Hardware (DO-254)
- IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (IEEE 7-4.3.2)
- International Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems (IEC 61508-2)

3 SUMMARIES OF SELECTED STANDARDS/PUBLISHED MATERIAL

Summaries have been provided for each of the 21 selected documents. The summaries are meant to highlight issues/solutions to designing safety-critical systems with FPGAs.

3.1 REGULATORY APPROACHES BY OTHER COUNTRIES AND AGENCIES

3.1.1 Japan

Transition and Current Status of NPP C&I System of BWRs in Japan

This document overviews the number and status of nuclear plants in Japan. In 2005, there were 53 plants in operation, 4 in construction, and 12 planned for construction. The document also presents the plan for controls and instrumentation (C&I) modernization using FPGA-based modules. The Power Range Neutron Monitor based on a one-time programmable FPGA has been recently developed and is currently undergoing quality assurance. Many other C&I systems under development will be using the FPGA technology.

3.1.2 France

PLD-Based Safety Critical Systems: An Introduction and Survey

This report was prepared by the University of Virginia (UVA) for Électricité de France. The first half of the report is a survey of FPGA devices. The report then discusses the use of mil-spec parts, test coverage (off-line and on-line), and triple-modular redundancy (TMR). Fault tolerance was also included and highly advocated due to degradation and/or disruption of the configuration bits. The report did raise concerns about the lack of independent fault containment regions, clocking, and power issues if replicated modular fault tolerance were to be achieved on an FPGA. Formal verification methods such as equivalence checking and model checking were recommended as good design practices. The report also identified the NASA ASIC study as well as citing DO-254 as the best guidance to date for defining the desired performance rather than prescribing how to achieve it.

3.1.3 Aerospace Industry

3.1.3.1 General findings

A Comparison of Radiation-Hard and Radiation-Tolerant FPGAs for Space Applications

The document compares rad-hard FPGA families, static random access memory- (SRAM-) based Xilinx FPGAs, and one-time programmable Actel FPGAs based on their performances for space applications. The performance characteristics compared are: total ionizing dose (TID) performance, single event upset (SEU) performance, SEU mitigation techniques, fan-out, operating temperature, operation clock speed, set-up and configuration time, power consumption, package quality, and known quality issues. The document also mentions Aeroflex and Atmel rad-hard FPGAs.

Formal Verification of Fault Tolerance in Safety-Critical Reconfigurable Modules

This document considers Esterel, a formal verification language for FPGA-based safety systems. It describes a design process that includes top-level design and verification as well as automatic code generation for synthesizable VHDL. The document states that this process reduces the likelihood of systematic faults. Also, it reveals how Esterel can be used for failure mode and effects analysis (FMEA) and for fault tree analysis (FTA).

Design, Test, and Certification Issues for Complex Integrated Circuits

This document mainly focused on ASICs but did contain some information on FPGAs like SRAM and Antifuse. It stated that as more sequential logic becomes available in a device, the more difficult that logic becomes to test. Single delays in FPGAs were discussed with causes listed as 1) signal wire characteristics, 2) programmable elements, 3) amount of cascaded logic cells, and 4) propagation delay of each logic cell.

FPGA Space Qualification Presentation

This document describes qualification of FPGA parts for space applications. The aerospace community and the United States government updated two main space qualification standards (MIL-STD-1546 and MIL-STD-1547) and published those updates as *Aerospace Technical Operating Report*. In 2006 the standards were updated again to include more stringent requirements and will be published again as MIL-STD-1546 and MIL-STD-1547. These documents will be used to qualify FPGA manufacturing processes as well.

Suitability of Reprogrammable FPGAs in Space Applications

This document investigates SEU issues related to FPGAs emphasizing Xilinx XC4000 and Virtex FPGAs, both rad-hard and general use versions. It briefly describes reprogrammable FPGA technology and its susceptibility to SEUs. The SRAM-based FPGAs have been used recently in applications such as avionics, space exploration, and high performance reconfigurable processors (different SEU mitigation techniques are reported for these applications). The most common is the TMR technique, but others include adding idle cycles for concurrent error detection, Hamming codes, and other parity codes, Built-in self-test (BIST), etc. To increase rad-hardness and reduce SEU sensitivity, most FPGA manufacturers use some kind of rad-hardened adjustment of their standard commercial foundry.

The document also describes three kinds of SEU in SRAM-based FPGAs. These are configuration memory upsets, used logic upsets, and architectural upsets [joint test action group (JTAG) upsets]. Several sensitive FPGA structures have been identified such as sequential and combinatorial logic, half-latches, lookup tables (LUTs), block random access memory (BRAM), digital clock manager (DCM), input/output (I/O) logic, and JTAG. The document covers many of the most common SEU mitigation techniques such as configuration memory protection, user logic protection, module-level protection, and gate-level protection. The document also reports some of the results of various SEU and TID tests performed on Virtex and XC400 FPGAs.

3.1.3.2 European Space Agency

VHDL Modeling Guidelines

This document defines acceptable practices for designing VHDL models and test benches used by the ESA. The purpose of these requirements is to ensure the models are of high quality so they can be efficiently used and maintained throughout the full life-cycle of a safety critical system. Some of the requirements are to use VHDL93, use the English language, limit the number of characters per line to 80, comment your design in detail within the code, use a defined code header at the beginning, and use assertions. The document suggests avoiding the buffer mode for the ports of top-level entity and single wait statements, in which a process statement with sensitivity list should be used.

Lessons Learned From FPGA Developments

This document contains information regarding problems encountered and lessons learned in the use of FPGAs involved in satellite missions from the ESA and NASA. This document has also been used by these agencies as an FPGA design guideline. However, the report only focuses on existing once-only programmable devices. The following topics were discussed as lessons learned: 1) transient performance of components not adequately accounted for in the design; 2) little to no documentation from FPGA designers and no established SEU requirements; 3) timing, static timing, clock skew, and low power designs are performed with ASICs and should be tested with FPGAs; 4) FPGA verification should not be done in isolation by the designer; and 5) specification should be established to define all relevant system configurations and characteristics to a level allowing FPGA device requirements to be derived.

The document concluded that employing FPGAs for critical use is only recommended when appropriate risk analysis has been performed and when the contractor can prove that the selected FPGA will fulfill its task in a given application and environment.

ASIC Design and Manufacturing Requirements

This document presents the requirements for ASIC (not FPGA) design used by ESA. Although FPGA design is not discussed, FPGA and ASIC design share many similarities. The document requires VHDL-based simulation at the architectural level, including the ASIC and other components on the board. Also, during the detailed design, VHDL should be used to simulate the ASIC's functionality. Later, during the prototype testing, the same VHDL test benches are used. The ASIC's set of specific design requirements include 1) use asynchronous reset rather than synchronous (ASIC's state should be completely deterministic after the reset); 2) be as synchronous as possible throughout the remaining design; 3) consider metastablity issues; 4) minimize the power and use clock control in the design; 5) address SEU issues; 6) avoid floating nodes; 7) avoid bus contention; 8) ensure there are no errors; and 9) eliminate unnecessary circuitry.

3.1.3.3 National Aeronautics and Space Administration

Independent Verification and Validation: First Year Summary Report for the Programmable Logic Devices Research

This document is related to SAIC Corporation's 2005 study for NASA's Goddard Software IV&V Facility regarding independent verification and validation (IV&V) of programmable logic devices (PLDs). It concentrates on verification and validation (V&V) of the VHDL code design, particularly syntax, I/O unknown states, coding style, unnecessary circuitry, dangerous semantics, etc.

The document examines four existing standards for software V&V: NASA-STD-8739.8, IEEE STD 1012-1998, IEEE STD 1076-2002, and DO-254. All of these documents mention the need for IV&V with regards to PLDs. The document stated that, "NASA has provided no clear guidance on the software aspects, design and development of PLDs, or how to assure safety, reliability, or quality of these hybrid devices."

Further, the document surveys formal PLD verification techniques, listing the most popular software tools for model checking, emphasizing the model-based verification of the VHDL programs where the design specification is used to test the designer's code. The document also lists most frequent "hot spots" in a VHDL design. The VHDL code examples point out design practices to be avoided.

A Preliminary Practitioner's Guide to Defect Detection in VHDL Based Designs

NASA's preliminary guide suggests an IV&V process for VHDL validation in FPGAs. The process includes artifacts (documents) collection, VHDL standard compliance analysis, pedagogical code examination, design artifact analysis, and final assessment.

Architectural Principles for Safety-Critical Real-Time Applications

This document discusses redundancy management, common mode/cause failures affecting multiple regions, fault avoidance, tolerance, removal, and exact versus approximate consensus. Stating that critical systems in many industries (such as the aerospace industry) are usually designed from scratch, it concludes that VHDL and a synthesis methodology should be integrated with formal specification and verification. It was also noted that for safety-critical applications, physical operational hardware faults no longer pose a major threat to dependability, but that the dominant threat is now common mode failures, for which no single theory can be applied and for which multidiscipline, multiphase defense is required.

3.1.4 Nuclear Industry

Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants

A Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI) met hoping to influence licensing agencies around the world to come to a consensus on common items so that it would be more efficient for vendors to supply instrumentation for a worldwide market.

AP1000 Instrumentation and Controls

Chapter 7 of this document discusses the descriptions and commitments pertaining to the primary instrumentation and control systems of the AP1000 design. The system uses microprocessor-based distributed digital systems to perform plant protection and control functions and safety monitoring. The active AP1000 systems are NOT classified as safety-related. Digital components for safety systems must be qualified for their intended application by either a 10 CFR Part 50, Appendix B quality assurance program or the item must be dedicated for use in the safety system as defined in 10 CFR Part 21. The NRC-approved EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” (1997) and BTP HICB-18 “Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems.”

Guidance on Software Reviews for digital Computer-Based Instrumentation and Control Systems

This document provides guidance on evaluating the life cycle of safety system software.

Embedded Digital System Reliability & Safety Analyses (NUREG/GR-0020)

NUREG/GR-0020 discusses dependability analysis of embedded digital systems as well as metrics that characterize dependability which are reliability, availability, and safety. This regulatory guide describes the most common axiomatic models such as Markov models, Petri nets, and fault trees. Each of these is implemented using commercially available software tools for dependability analysis.

This regulatory guide identifies methods that can be used to achieve dependability: defense in depth, redundancy, diversity, and robustness. The most important dependability parameters are failure rate, repair rate, and coverage. The document classifies four types of redundancy: hardware, software, time, and information redundancy. Diversity is classified as human, design, software, functional, equipment, and signal diversity.

In discussing the embedded digital systems reliability and safety analysis, the document recommends that the hardware and software in these systems be analyzed as integral parts of the systems and not separately, as is common practice. However, the document does not address any methods specific to the digital systems, but only suggests that the existing methodology be used for digital systems as well.

3.1.5 AUTOMOTIVE INDUSTRY

Reliability Considerations for Automotive FPGAs

This paper focuses on the fundamental importance of technology selection and its relationship to overall system reliability relative to the automobile industry. Cause and cure are emphasized. The following topics are discussed: temperature as a primary stress factor in semiconductor failure, neutron-induced soft and firm errors, tamper resistance in automotive FPGAs, and time-dependent dielectric breakdown (TDDB). Reliability problems frequently encountered by FPGAs are typically due to one of four root causes: 1) the packaging technology, 2) assembly technology, 3) environmental overstress, 4) electrostatic discharge (ESD) Exposure to high temperature exacerbates these types of problems. Antifuse architectures are superior in their tolerance to extended temperature exposures.

This document discusses SEUs and the fact that it is not possible to shield against high-energy neutrons, so designers must either account for the effects of such neutrons or use neutron-resistant technology. Of the three main FPGA technologies, antifuse, Flash, and SRAM, only antifuse and Flash are immune to the effects of neutron-induced soft and firm errors. SRAM-based products are the least secure of all technologies.

3.2 EXISTING STANDARDS

Design Assurance Guidance for Airborne Electronic Hardware (DO-254)

The DO-254 standard establishes assurance guidelines for complex hardware systems that use FPGAs, complex programmable logic devices (CPLD), and ASIC. This standard is concerned with the entire hardware design life cycle —planning, hardware design, validation, verification, configuration management, process assurance, and certification. However, the standard considers FPGAs as purely hardware devices ignoring the fact that FPGA design involves Hardware Design Language (HDL) programming and simulation typical for software systems. Also, the standard does not include any details regarding safe FPGA design practices, acceptance criteria, or licensing procedures that are necessary parts of a regulatory document for I&C in nuclear plants.

DO-254 defines five levels of safety criticality from Level A, the most critical, to Level E, not critical. Also, the standard requires the assessment of the hardware safety using the following principles: 1) circuit or component redundancy, 2) separation or electrical isolation between circuits or components, 3) dissimilarity between circuits or components, 4) monitoring of circuit or components, 5) protection or reconfiguration mechanisms, 6) allowed failure rates and probabilities for the circuit and component random failures and latent failures, 7) limitation of usage or installation, and 8) prevention and management of upsets and upset recovery. However, the document does not address the specific failure modes for FPGA-based safety systems.

IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (IEEE 7-4.3.2)

IEEE 7-4.3.2 supplements IEEE 603 by addressing the use of computers as part of safety systems in nuclear power plants. This standard includes 1) software quality (software tools, V&V [IEEE 1012-1998], IV&V requirements, software configuration management, and software program risk management); 2) data communication between safety systems and safety to non-safety systems –(performance of the safety function shall not be inhibited); and 3) common cause failure criteria (guidance on performing an engineering evaluation of software common-cause failures).

International Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems (IEC 61508-2)

IEC 61508 is a standard that provides a generic approach intended for all industries using electrical/electronic/programmable electronic components to perform safety-related activities. This standard discusses safety requirements and provides a list of specifications that must be met. It also contains a list for safety integrity requirements.

The standard states that using static, dynamic, and failure analysis should reduce the test cases needed and that there must be an estimated rate of failure. Finally, it is stated that it is practically impossible to list all physical failures of complex hardware. One reason given is the difference of determining the relationship between failures. Another reason is that there is a greater contribution of systematic failures in contrast to random failures when complex hardware and software is used. Failures should also be categorized in terms of failures caused by faults, before or during system installation, and failures caused by faults or human errors, after system installation.

4 DOCUMENT EVALUATION/COMMENTS

It is evident from reviewing the documents discussed in this report that there is no ready-to-use regulatory guidance directly applicable to the FPGA-based safety-critical system design. However, DO-254 does represent a good overall approach for design of hardware-based safety-critical systems. DO-254 considers all phases of the hardware-design life cycle including requirement capture, conceptual design, detailed design, implementation, and production transition. For each of these phases, it describes how to implement V&V, configuration management, process assurance, and certification. It also describes how to apply the assessment and qualification process for the software/hardware tools used during design.

IEEE 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," concentrates on the software side of safety-critical system design using digital computers. It can be used as guidance for developing V&V planning, configuration management, requirement traceability, failure modes and effects, and environmental qualifications during the software design. Generally, the software side of the FPGA design more closely resembles the assembly language programming in computers and only recently have higher-level languages been used for FPGA design. The software design in digital computers and microprocessors has almost exclusively involved the use of high-level programming languages and powerful compilers.

Many reviewed documents recognize the need for a specific design approach when considering FPGAs for safety-critical systems. This is particularly elaborated in documents from the space exploration community as well as in the transportation and auto industry. This specific design approach is due to the unique FPGA characteristic that requires concurrent and interdependent hardware and software design paths.

The reviewed documents identify a large number of safe FPGA design practices including hardware and software design. The hardware design practices include issues such as board-level design, FPGA logic design, SEEs in FPGAs, programming, etc. Software design practices include using schematic entry for time-critical design, avoiding unsafe and ambiguous VHDL and Verilog programming structures, full coverage during the simulation and hardware verification, using formal methods for V&V, etc.

Thus far, the FPGA design methodology used by the manufacturers of safety-critical systems has been based on mainstream FPGA design tools not certified for use in safety-critical design. The FPGA design verification is done by exhaustive simulation-based testing. This offered sufficient confidence in the design, primarily because such testing involves relatively simple designs with full-simulation coverage capability.. . However, the growing complexity of FPGA designs in safety-critical systems is likely to require a different design methodology based on more formal verification methods. Furthermore, the mainstream FPGA design tools would need to be certified for use in safety-critical systems.

Recently vendors have started offering FPGA-based systems for I&C in nuclear plants. From the available documentation, these systems use FPGAs generally for relatively simple tasks. Most popular are one-time programmable FPGAs with built-in redundancy for SEE mitigation. Also, some European systems use CPLDs instead of FPGAs, which are appropriate for simple logic subjected to benign environments. SRAM-based reprogrammable FPGAs are widely used in aerospace and military applications where high-density FPGAs and reprogrammability are needed. However, these FPGAs require a different set of mitigation techniques to address SEEs in the configuration and user logic.

5 CONCLUSION

In conclusion, even though there are no FPGA-specific regulatory documents for safety-critical systems at this time, all the related documents reviewed clearly expressed a need for such documents. One could argue that because FPGAs represent a higher level of integration of existing digital systems, no special regulatory documents are needed. However, the inherent complexity and ever-increasing size and functional diversity of FPGAs require a specific set of design practices when FPGAs are used in safety-critical systems.

APPENDIX: RESULTS OF INTERNET SEARCH FOR TECHNICAL STANDARDS RELATED TO FPGA DESIGN

R. Katz (2005, Jul.) “This Is What We Find In This Stuff: A Designer Engineer's View,” Presentation at the FY2005 Software/Complex Electronic Hardware Standardization Conference, Norfolk, Virginia, July 26–28, 2005. http://www.klabs.org/richcontent/Tutorial/MiniCourses/stuff_faa_nasa_2005/index.htm

G. Chen, F. Li, M. Kandemir and I. Demirkiran, “Increasing FPGA Resilience Against Soft Errors Using Task Duplication,” ASP-DAC-2005, pp. 924–927. http://ieeexplore.ieee.org/iel5/9883/31416/01466490.pdf

John Lach, William H. Mangione-Smith, and Miodrag Potkonjak, “Enhanced FPGA Reliability Through Efficient Run-Time Fault Reconfiguration,” IEEE Transactions on Reliability, vol. 49, No. 3, September 2000 pp. 296–304. http://ieeexplore.ieee.org/iel5/24/19750/00914546.pdf?arnumber=914546

Chandru Mirchandani, “Using Software Rules To Enhance FPGA Reliability,” P226/MAPLD2005, September 2005. http://www.klabs.org/mapld05/presento/226_mirchandani-bof-w.ppt

D. Czajkowski, D. Strobel, P. Samudrala, and M. Pagey, “Radiation Hardened, Ultra Low Power, High Performance Space Computer Leveraging COTS Microelectronics With SEE Mitigation,” Space Micro Inc. (MAPLD2005/138). http://www.klabs.org/mapld05/presento/138_czajkowski_bof-m.pdf

Howard Bogrow, “The Continued Evolution of Re-Configurable FPGAs for Aerospace and Defense Strategic Applications,” Xilinx (MAPLD2005/176). http://www.klabs.org/mapld05/presento/176_bogrow_p.ppt

Carl Carmichael, Brendan Bridgford, and Xilinx, Inc., “A Cost/benefit Framework for Evaluating Re-configurable FPGA SEU mitigation Techniques,” Xilinx (MAPLD2005/194). http://www.klabs.org/mapld05/presento/194_bridgford_p.ppt

Carl Carmichael, Sana Rezgui, Gary Swift, Jeff George, & Larry Edmonds, “SEE Validation of SEU Mitigation Methods for FPGAs,” California Institute of Technology, Jet Propulsion Laboratory, and National Aeronautics and Space Administration (P201-L/MAPLD2005). http://www.klabs.org/mapld05/presento/201_carmichael_bof-l.ppt

Sajid Baloch, Tughrul Arslan, and Adrian Stoica, “Design of a 'Single Event Effect Mitigation Technique for Reconfigurable Architectures", MAPLD 2005, Submission 1024, Session P and L. http://www.klabs.org/mapld05/abstracts/1024_baloch_a.pdf

Department of Defense, “Test Method Standard Microcircuits,” MIL-STD-883E, December 1996. http://atlas.web.cern.ch/Atlas/GROUPS/FRONTEND/WWW/RAD/RadWebPage/StandardMeth/milstd~1.pdf

Advisory Circular, “RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance For Airborne Electronic Hardware,” June 2005. http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/7aab5bad14f9417885256a35006d56b0/6d4ae0bf1bde3579862570360055d119/$FILE/AC%2020-152.pdf

Terrence Leier and Robert Haug, “Best Practices in Complex Electronic Hardware Development,” July 2005.

Thomas Phan, "Special Delegations for Complex Hardware & TSO Software,” Presented to 2005 National Software and Complex Electronic Hardware Standardization Conference, Norfolk, Virginia, July 2005. http://klabs.org/richcontent/conferences/faa_nasa_2005/presentations/tuesday_general.htm

Memorandum from Kim Smith, Manager of Small Airplane Directorate at FAA, "Applying Advisory Circular 20-152, 'RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware,' to Title 14 Code of Federal Regulations, Part 23 Aircraft; PS-ACD100-2005-50001.” http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgPolicy.nsf/97a612e22b32398d85256b7500496a9a/cf51a956f07b0c208625727c006745ca/$FILE/PS-ACE100-2005-50001%20final.pdf

Akira Fukumoto, Toshiba Corporation, “Transition and Current Status of NPP C&I System of BWRs in Japan.” http://entrac.iaea.org/I-and-C/TWG_NPP_CI_2005_05/Presentations%5CJapan-Fukumoto.pdf

Suresh Srinivasan, Aman Gayasen, N. Vijaykrishnan, M. Kandemir, Y. Xie, M.J. Irwin, “Improving Sof-Error Tolerance of FPGA Configuration Bits,” Department of Computer Science and Engineering, Pennsylvania State University, 2004. http://www.cse.psu.edu/~degalaha/paper/iccad.pdf

H. Helstrup ,V. Lindenstruth , S. Martens , L. Musa , J. Nystrand ,E. Olsen , D.Rohrich , K. Roed, B. Skaali , M. Stockmeier ,H. Tilsner , K. Ullaland ,J. Wikne, “Irradiation tests of the ALTERA SRAM based FPGA and fault tolerant design concepts.” http://lhc-electronics-workshop.web.cern.ch/LHC-electronics-workshop/2003/sessionsPDF/Eleccal/ROED.PDF

Ghazanfar Asadi, Mehdi B. Tahoori, “An Analytical Approach for Soft Error Rate Estimation in Digital Circuits.” http://www.ece.neu.edu/groups/trg/index_files/papers/ser/iscas05.pdf

Ghazanfar Asadi, Mehdi B. Tahoori, “Soft Error Rate Estimation and Mitigation for SRAM-Based FPGAs,” 2005. http://www.ece.neu.edu/groups/trg/index_files/papers/serfpga/fpga05final.pdf

Goddard Space Flight Center NASA Advisory, "Application Note on Grounding the MODE Pin in Actel Field Programmable Gate Arrays,” November 2002. http://klabs.org/richcontent/User_Notes/Actel/na-gsfc-2003-02.pdf

Goddard Space Flight Center NASA Advisory, "TRST* and the IEEE JTAG 1149.1 Interface,” February 2004. http://klabs.org/richcontent/maplug/notices/na-gsfc-2004-04.pdf

NASA Independent Verification and Validation Facility, *NASA IV&V 2005*. http://www.nasa.gov/centers/ivv/about/policyplans.html

Ramin Roosta, "A Comparison of Radiation-Hard and Radiation-Tolerant FPGAs for Space Applications,” NASA Electronic Parts and Packaging Program, December 2004. http://nepp.nasa.gov/docuploads/3C8F70A3-2452-4336-B70CDF1C1B08F805/JPL%20Rad-Tolerant%20FPGAs%20for%20Space%20Applications.pdf

Commision on Engineering and Technical Systems, "Dedication of Commercial Off-the-Shelf Hardware and Software,” Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues (1997). http://www.nap.edu/openbook.php?isbn=0309057329&page=71

Actel, "Overview of iRoC Technologies' Report "Radiation Results of the SER Test of Actel, Xilinx and Altera FPGA Instances,” 2004. http://www.actel.com/documents/OverviewRadResultsIROC.pdf iRoC Technologies, "Radiation Results of the SER Test of Actel, Xilinx and Altera FPGA Instances," October 2004. http://www.actel.com/documents/RadResultsIROCreport.pdf

iRoC Technologies, "White Paper on VDSM IC Logic and Memory Signal Integrity and Soft Errors," January 2002.

Jerker Hammarberg and Simin Nadjm-Tehrani, "Formal Verification of Fault Tolerance in Safety-Critical Reconfigurable Modules," August 2004. http://www.ida.liu.se/~rtslab/publications/2005/STTT0152.pdf

Gaisler Research, "Lessons Learned from FPGA Developments," Technical Report, September 2002. http://www.gaisler.com/doc/fpga_001_01-0-2.pdf

John Lach, Scott Bingham, Carl Elks, Travis Lenhart, Thuy Nguyen, and Patrick Salaun, "Accessible Formal Verification for Safety-Critical FPGA Design," MAPLD 2005/241. http://klabs.org/mapld05/presento/241_lach_p.ppt

Carl Elks and Barry Johnson, "PLD-based Safety Critical Systems: An Introduction and Survey," Final Technical and Scientific Report, February 2004.

John Lach, Scott Bingham, Travis Lenhart, Thuy Nguyen, and Patrick Salaun, "RAFFIA- Reliable ASIC/FPGA-based Solutions for I&C Applications."

John Lach, "Integrated Circuits and Systems Design Methodologies," Research Program Overview. http://www.ee.virginia.edu/graduate/Lach_research_overview.pdf

University of Virginia, "Embedded Digital System Reliability and Safety Analyses," NUREG/GR-0020, February 2001.

Dr. Wagih Abdel-Kader, "Radiation Induced Effects in Semiconductor Devices" part 1–3.

International Atomic Energy Agency, "Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants," December 2002. http://www-pub.iaea.org/MTCD/publications/PDF/te_1327_web.pdf

L. Harrison and B. Landell, "Design, Test, and Certification Issues for Complex Integrated Circuits," DOT/FAA/AR-95/31, August 1996. http://klabs.org/richcontent/verification/faa/ar-95-31-ceh.doc

European Space Research and Technology Center, "VHDL Modelling Guidelines," Approved by R. Creasey and R. Coirault, ASIC/001, Issue 1, September 1994. http://www.eda.org/rassp/vhdl/guidelines/ModelGuide.pdf

European Space Research and Technology Center, "ASIC Design and Manufacturing Requirements," Prepared by S. Habinc and P. Sinander, WDN/PS/700, Issue 2, October 1994. http://www.eda.org/rassp/vhdl/guidelines/DesignReq.pdf

IEEE Std 7-4.3.2 – 2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

AP1000 Design Control Document Tier 2, Chapter 7, "Instrumentation and Controls." http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1793/chapter7.pdf

Branch Technical Position HICB-14, “Guidance on Software Reviews for Digital Computer–Based Instrumentation and Control Systems.”

Jonathan Tillack, Lori Kaufman, Karthik Kannan, Barry Johnson, “Design Standards and their Application to the Digital Retrofit of Existing Analog Safety-Critical Systems,” 2000 Proceedings Annual Reliability and Maintainability Symposium. http://ieeexplore.ieee.org/iel5/6628/17683/00816332.pdf

Ray DiSandro, Ray Torok, “Generic Qualification of Digital Components.”

“Generic Qualification of Digital Components for Nuclear Applications: A Low-Cost Approach to Qualifying New Digital I&C Components for Nuclear Plant Use, Especially in Safety Systems,” April 2002.

Matthew Chiramal, “Application of Commercial-Grade Digital Equipment in Nuclear Power Plant Safety Systems.” http://ieeexplore.ieee.org/iel5/7654/20915/00969772.pdf

International Atomic Energy Agency, “Managing modernization of nuclear power plant instrumentation and control systems,” IAEA-TECDOC-1389, February 2004. http://www-pub.iaea.org/MTCD/publications/PDF/te_1389_web.pdf

Matthew Chiramal, “Regulatory Framework for Digital Instrumentation and Control Systems in Nuclear Power Plants,” MIT Workshop on Safety-Critical Software and Safety, February 2001. http://sunnyday.mit.edu/safety-club/chiramal.rtf

Lawrence Livermore National Laboratory, “Review Templates for Computer-Based Reactor Protection Systems,” NUREG/CR-6680, UCRL-ID-139344, August 2000. http://adamswebsearch2.nrc.gov/idmws/doccontent.dll?library=PU_ADAMS^PBNTAD01&ID=003960624

Hluboka nad Vltavou, “CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems,” NEA/CSNI/R(2002)4, May 2002. http://www.nea.fr/html/nsd/docs/2002/csni-r2002-4.pdf

Nihal Kececi and Mohammad Modarres, “Software Development Life Cycle Model to Ensure Software Quality.” http://www.cse.ohio-state.edu/~kirschen/Research/psam-paper2.PDF

M. Hecht and H. Hecht, “Digital Systems Software Requirements Guidelines.”

“Safety Evaluation by the Office of nuclear Reactor Regulation – Topical Reports 7286-545 and 7286-546,” Project #709, December 2001. http://adamswebsearch2.nrc.gov/idmws/doccontent.dll?library=PU_ADAMS^PBNTAD01&ID=004042634

International Standard, IEC 61508-2, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 2: Requirements for Electrical/Electronic/ Programmable Electronic Safety-Related Systems.”

Jaynarayan Lala and Richard Harper, “Architectural Principles for Safety-Critical Real-Time Applications,” Proceeding of IEEE, vol.82, No. 1, January 1994. http://ieeexplore.ieee.org/iel1/5/6554/00259424.pdf?arnumber=259424

Larry Harzstark, “FPGA (Field Programmable Gate Array) Space Qualification Presentation,” December 2005. http://www.aero.org/conferences/mrqw/2005-papers/VII-1%20Harzstark.ppt

Douglas Sheldon, “Integrated Qualification Strategies for FPGAs,” December 2005. http://www.aero.org/conferences/mrqw/2005-papers/VII-2%20Sheldon.ppt

Michael Wirthlin, Brian Pratt and Keith Morgan, “The Challenges and Benefits of Partial Mitigation of FPGAs.” http://www.aero.org/conferences/mrqw/2005-papers/VII-3%20Wirthlin.ppt

iRoC Technologies, “Answers to Frequently Asked Questions Regarding iRoC’s Testing Methodology for SRAM-based FPGAs,” June 2004.

Michael Wirthlin, Eric Johnson, Nathan Rollins, Michael Caffrey, and Paul Graham, “The Reliability of FPGA Circuit Designs in the Presence of Radiation Induced Configuration Upsets,” Proceeding of IEEE Symposium on Field-Programmable Custom Computing Machines, 2003.

EPRI Working Group on Use of Commercial Digital Equipment in Nuclear Safety Applications with MPR Associates, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for nuclear Safety Applications,” TR-106439, October 1996.

Actel White Paper, “Reliability Considerations for Automotive FPGAs,” September 2003. http://www.actel.com/documents/AutoWP.pdf

Science Applications International Corporation, “Independent Verification and Validation (IV&V) First Year Summary Report for the Programmable Logic Devices Research,” SAIC-PLD-0002, ISTO-06-98-133, September 2005.

United States Nuclear Regulatory Commission, “Briefing on Digital Instrumentation and Control,” November 2006.

L. Sterpone and M. Violante, “A design flow for protecting FPGA-based systems against single event upsets,” Proceedings of IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, 2005. http://ieeexplore.ieee.org/iel5/10366/32969/01544543.pdf?arnumber=1544543

James Cercone, Mike Beims, Richard Grigg, and Jack Horner, “A Preliminary Practitioner’s Guide to Defect Detection in VHDL Based Designs.”

Gaisler Research, “Suitability of reprogrammable FPGAs in space applications,” FPGA-002-01, Version 0.4, September 2002. http://www.gaisler.com/doc/fpga_002_01-0-4.pdf

Adrian Hilton, Gemma Townson, and Jon Hall, “FPGAs in Critical Hardware/Software Systems,” Technical Report No: 2003/01, 2003.

Adrian Hilton and Jon Hall, “High-Integrity Interfacing to Programmable Logic with Ada,” Ada-Europe International Conference, June 2004. http://www.praxis-his.com/sparkada/pdfs/hilton_hall_adaeurope.pdf

Moore Industries, “IEC 61508 Fact Sheet.” http://www.mooreindustries.com/products/data_sheets/iec_61508.pdf

“Functional Safety and IEC 61508 – A Basic Guide,” November 2002. http://www.nepss.org/PSES/IEC61508basicguide.pdf

NASA, “Software Assurance Standard,” NASA-STD-8739.8, July 2004. http://www.hq.nasa.gov/office/codeq/doctree/87398.pdf

Rod Barto, “Suggestions for FPGA Design Presentation.”

Carl Elks, John Lach, and Barry Johnson, “PLD-based Safety Critical Systems: Task 1 and 2 – Assessment, Practices and Design,” November 2006.

Carl Elks, Yang Yang Yu, and Barry Johnson, “Quantitative Safety Assessment for Safety-Critical I&C Systems.”

Scott Bingham and John Lach, “Accessible Formal Verification for Safety-Critical Hardware Design: The Library Approach RAFFIA 1.”

John Lach, “Dependable Hardware Systems Research Program Overview.”

John Lach, Scott Bingham, Carl Elks, Travis Lenhart, Thuy Nguyen, and Patrick Salaun, “Accessible Formal Verification for Safety-Critical FPGA Design,” MAPLD 2005/241.