Introduction of Safety Digital I&C System Based on FPGA Technology

Wangjiacheng, Chief Engineer of R&D State Nuclear Power Automation System Engineering Company

wangjiacheng@snpas.com.cn
086-18930175216
知识产权声明

本文件的知识产权属国家电力投资集团公司及其相关产权人所有，并含有其保密信息。对本文件的使用及处置应严格遵循获取本文件的合同及约定的条件和要求。未经国家电力投资集团公司事先书面同意，不得对外披露、复制。

Intellectual Property Rights Statement

This document is the property of and contains proprietary information owned by SPIC and/or its related proprietor. You agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you. No disclosure or copy of this document is permitted without the prior written permission of SPIC.
1: FPGA Technology Introduction
2: R&D Achievements
3: Current Research Direction
FPGA Technology Introduction

Background
Field-programmable gate arrays (FPGAs) are gaining increased attention worldwide for application in nuclear power plant (NPP) instrumentation and control (I&C) systems, particularly for safety applications. The use of FPGAs might reduce complexity and the associated burden of gaining regulatory approval and provide better protection against obsolescence compared to conventional microprocessor-based systems.
Programmable logic devices (PLDs) are another alternative for use in nuclear applications, having been widely used in many industrial, military and aerospace applications for years.

PLDs fit into the overall landscape of electronic hardware technologies, including conventional technologies, ASICs and microprocessors. PLDs contain arrays of logic elements that can be interconnected by the user to perform the functions required for a particular application. The first to become available were simple PLDs, which include programmable logic arrays (PLAs) and programmable array logic (PAL).
FPGA Technology Introduction

Complex PLDs (CPLDs) evolved from PALs – they essentially combine multiple PALs on a single chip, with ability to interconnect them to perform more complex functions.

FPGAs also can be considered PLDs, but they have a different internal architecture, FPGAs use “gate arrays” as opposed to “logic arrays” among other differences. FPGAs available today contain ten-millions of gates (logic elements or configurable logic blocks) that can be interconnected to perform functions with a wide range of complexity.
FPGA Technology Introduction

- Advantages of FPGA Technology
  
  - Reduced Complexity

Note: From EPRI1022983

©SPIC 2018. All Rights Reserved.
FPGA Technology Introduction

- Advantages of FPGA Technology

  - Long-Term Support and Portability
    - long term commitments (possibly with other industries such as aerospace or the military)

Note: From EPRI1022983
FPGA Technology Introduction

- Advantages of FPGA Technology

  - **Application as a Diverse**
    - Microprocessors Based I&C System for Control System

  - **Verifiability**
    - Lower complexity
    - segregate independent functions
    - parallelism
    - See behavior Directly
## FPGA Technology Introduction

### Comparison of FPGAs and Other I&C Technologies

<table>
<thead>
<tr>
<th>NO</th>
<th>Technology</th>
<th>Design Process</th>
<th>End Product</th>
<th>Focus of Safety Justification</th>
<th>Longevity of Support</th>
<th>Functional Capability Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Conventional hardware (Relays, analog electronics, discrete digital electronics)</td>
<td>Hardware design (Conventional hardware design and QA)</td>
<td>Hardware (Discrete components)</td>
<td>Hardware design review (Conventional hardware design review; review of design controls/QA; functional testing)</td>
<td>Long (Was long, but now obsolete)</td>
<td>Low (Difficult to do complex algorithms &amp; self-testing features; limited information output)</td>
</tr>
<tr>
<td>2</td>
<td>FPGA with flat hardware logic (Flat hardware logic implementation in an FPGA chip)</td>
<td>Software-assisted hardware design (Electronic hardware design and V&amp;V, assisted by software tools, possibly applying formal methods)</td>
<td>Hardware (Integrated circuit)</td>
<td>Software-like hardware design process review (Review of design and V&amp;V processes similar to software development; review hardware design; functional testing)</td>
<td>Long (Close to conventional hardware, with promise to extend design portability even further)</td>
<td>Moderate to High (Can implement self-testing in parallel, independent of logic processing)</td>
</tr>
<tr>
<td>3</td>
<td>Conventional Microprocessor-based systems (Microcontrollers, PLCs, DCS, etc.)</td>
<td>Software design (Software design and QA, assisted by software tools)</td>
<td>Software and hardware (Conventional microprocessor plus run-time software)</td>
<td>Software design process and design review (Software development and V&amp;V process review per software engineering standards)</td>
<td>Short (Microprocessors and base software have much shorter life cycle than conventional hardware)</td>
<td>High to Very High (Can handle complex algorithms, self-testing, information display, and complex HMI)</td>
</tr>
</tbody>
</table>
FPGA Technology Introduction

Thee Major Kinds of FPGA Technology

**SRAM** – static random access memory or SRAM is re-writable, which means that the implemented functionality can be modified without physically replacing the FPGA component. Because it is volatile memory, with SRAM the programming is not retained by the circuit on a loss of power. Also, a power glitch may alter the FPGA programming (interconnection grid, CLBs, I/O blocks). As a result, measures may need to be taken to protect against power glitches and other single-event upsets (SEUs) when SRAM is used.

**Flash and EPROM** – erasable programmable read-only memory (EPROM) and flash technologies are re-writable and non-volatile. Flash is a modern derivative of the older, slower EPROM technology. In both cases the FPGA programming is unaltered by power glitches. Flash and EPROM also may provide greater inherent immunity to SEUs as compared to SRAM.
FPGA Technology Introduction

Thee Major Kinds of FPGA Technology

**Anti-fuse** – this technology is non-rewritable and non-volatile. A contact between two wires of the interconnection grid is created by sending a high current through the wires. Rather than breaking a connection or fuse to form the current flow, the connection is created between two logic blocks by means of (for example) heated nickel-alloy links, thus the name “anti-fuse.”

### Alpha Radiation Test Results Summary

<table>
<thead>
<tr>
<th>FPGA</th>
<th>Technology</th>
<th>Equivalent Failure-in-Time (FIT) Rate</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Low-Alpha Mold Compound (0.001 α/cm²·hr)</td>
<td>Standard Mold Compound (0.04 α/cm²·hr)</td>
</tr>
<tr>
<td>Actel AX1000 1 M Gate</td>
<td>0.15 μm Antifuse</td>
<td>No failures detected</td>
<td>No failures detected</td>
</tr>
<tr>
<td>Actel APA1000 1 M Gate</td>
<td>0.22 μm Flash</td>
<td>No failures detected</td>
<td>No failures detected</td>
</tr>
<tr>
<td>Actel A3PE600 600 k Gate</td>
<td>0.13 μm Flash</td>
<td>No failures detected</td>
<td>No failures detected</td>
</tr>
<tr>
<td>Vendor1 SRAM FPGA 3 M Gate</td>
<td>0.15 μm SRAM</td>
<td>140 FITs</td>
<td>5,600 FITs</td>
</tr>
<tr>
<td>Vendor1 SRAM FPGA 1 M Gate</td>
<td>90 nm SRAM</td>
<td>260 FITs</td>
<td>10,400 FITs</td>
</tr>
<tr>
<td>Vendor2 SRAM FPGA 1 M Gate</td>
<td>0.13 μm SRAM</td>
<td>100 FITs</td>
<td>4,000 FITs</td>
</tr>
</tbody>
</table>
**FPGA Technology Introduction**

**Neutron Radiation Test Results Summary**

<table>
<thead>
<tr>
<th>FPGA</th>
<th>Technology</th>
<th>Equivalent Functional FIT Rates per Device</th>
<th>Ground-Level Applications</th>
<th>Commercial Aviation</th>
<th>Military Aviation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sea Level 5,000 Feet 30,000 Feet 60,000 Feet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actel AX1000 1 M Gate</td>
<td>0.15 μm Antifuse</td>
<td>No failures detected</td>
<td>No failures detected</td>
<td>No failures detected</td>
<td>No failures detected</td>
</tr>
<tr>
<td>Actel APA1000 1 M Gate</td>
<td>0.22 μm Flash</td>
<td>No failures detected</td>
<td>No failures detected</td>
<td>No failures detected</td>
<td>No failures detected</td>
</tr>
<tr>
<td>Actel A3PE500 600 k Gate</td>
<td>0.13 μm Flash</td>
<td>No failures detected</td>
<td>No failures detected</td>
<td>No failures detected</td>
<td>No failures detected</td>
</tr>
<tr>
<td>Vendor1 SRAM FPGA 3 M Gate</td>
<td>0.15 μm SRAM</td>
<td>1,150 FITs</td>
<td>3,900 FITs</td>
<td>170,000 FITs</td>
<td>540,000 FITs</td>
</tr>
<tr>
<td>Vendor1 SRAM FPGA 1 M Gate</td>
<td>90 nm SRAM</td>
<td>320 FITs</td>
<td>1,100 FITs</td>
<td>47,000 FITs</td>
<td>150,000 FITs</td>
</tr>
<tr>
<td>Vendor2 SRAM FPGA 1 M Gate</td>
<td>0.13 μm SRAM</td>
<td>460 FITs</td>
<td>1,600 FITs</td>
<td>67,000 FITs</td>
<td>220,000 FITs</td>
</tr>
<tr>
<td>Vendor2 SRAM FPGA 1 M Gate</td>
<td>90 nm SRAM</td>
<td>730 FITs</td>
<td>2,500 FITs</td>
<td>108,000 FITs</td>
<td>346,000 FITs</td>
</tr>
<tr>
<td>Vendor2 SRAM FPGA 2 M Gate</td>
<td>90 nm SRAM</td>
<td>1,600 FITs</td>
<td>5,500 FITs</td>
<td>236,000 FITs</td>
<td>751,000 FITs</td>
</tr>
</tbody>
</table>

**Consider to use Flash and EPROM FPGA for Safety Platform!**
FPGA Technology Introduction

Note: From EPRI1022983

©SPIC 2018. All Rights Reserved.
FPGA Technology Introduction

Major Standard and Guidance:
IEEE Std. 1012 : Standard for Software Verification and Validation

NUREG/CR-7006 : Review Guidelines for Field Programmable Gate Arrays in Nuclear Power Plant Safety Systems

IEC 62566 : Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions”
1 : FPGA Technology Introduction
2 : R&D Achievements
3 : Current Research Direction
R&D Achievements

- **SNPAS and LMGI** - Nuclear Protection and Control (NuPAC)® **Platform** (Flash Based FPGA) - Plan to used in RTS and ESFAS for CAP1400
- **Westinghouse** - Component Interface Modules (EPROM Based FPGA) - Used in ESFAS for AP1000
- **Westinghouse** - Advanced Logic System® (ALS) - Used in Wolf Creek Main Steam and Feedwater Isolation System (MSFIS)
- **DOOSAN** - HFC-FPGA Product - Used in ESFAS in new plant
- **Radiy** - RadICS Platform - (Base SRAM and Flash FPGA) - RTS and ESFAS in Ukraine and Bulgaria for VVER
- **Hitachi** - Digital power range neutron monitor (PRNM) system (Anti-fuse type based FPGAs) - Used in boiling water reactor (BWR) plants in Japan.
- **Rolls Royce Civil Nuclear (RRCN)** - Slave Logic Units (Flash-based FPGAs) - Used in Rod Control System in France
- **OPG** - Digital Control Computer Upgrade (SRAM-based FPGAs) in CANDU plant
R&D Achievements

- **NuPAC Platform**

The NuPAC platform is a new generation of digital safety instrumentation platform based on Field Programmable Gate Array (FPGA) technology jointly developed by State Nuclear Power Automation System Engineering Company (SNPAS) and Lockheed Martin Global, Inc. (LMGI). Its unique system architecture design makes safety, Reliability, testability, verifiability can be fully improved. The new system has been the first safety-level digital instrumentation and control platform that is accredited by the China and USA Nuclear Regulatory Commission.

▲ Based on EPRI 107330 design
▲ Reduce the risk of software common cause failure:
  · No microprocessors, operating systems and pre-development software;
  · Pure hardware system;
▲ The system can be fully verified
▲ System behavior is deterministic
▲ Equipment classification: Class 1E（IEEE 603-1998）
R&D Achievements

• **Product typical structure**

  The NuPAC platform is functionally and physically similar to a commercially available programmable logic controller (PLC). However, the decentralized architecture of FPGAs offers a unique safety-level platform architecture that is similar to hardware-based solutions in existing nuclear power plants.
Product typical structure
NuPAC platform architecture is based on configurable modules as the core components, these components are called Generic Logic Module (GLM). The GLM consists of a carrier card, a logic mezzanine and up to eight I/O. Each GLM has input/output processing, custom control logic, diagnostic and data communications capabilities.
R&D Achievements

Product typical structure

Bi-stable Processing Logic

Mash Network and Point And Point between GLMS
R&D Achievements

- Generic Logic Module
R&D Achievements
R&D Achievements

- Chassis
R&D Achievements

- Logic Mezzanine

The programmable logic devices include two FPGAs, which are designated the Core PLD and the Application Specific PLD (ASPLD).
R&D Achievements

Programmable Logic Structure

The logic mezzanine contains two FPGA processing units the core programmable logic device (PLD) and application-specific PLD (ASPLD).
R&D Achievements

Programmable Logic Development Process
R&D Achievements

Programmable Logic Verification & Validation Test Method

Constrained Random Verification (CRV)

Functional Coverage 100%

Code coverage 100% with Justification:

- Statement;
- Branches;
- Expression;
- Condition;
- Finite State Machine (FSM);
R&D Achievements

国家核安全局

HAF601民用核安全设备批复
（国核安发[2016]312号）
R&D Achievements

Safety Evaluation Report
(TAC NO. ME7900)
R&D Achievements

IV&V TUV ISTec

(SNPAS-SWV&V-WI-201708-01)

Assessment Conclusion: The assessment has been passed without procedural remainders. The presented software verification and validation (V&V) procedures of SNPAS are suitable for a qualified V&V process for safety software according to the applicable procedural and quality requirements of the standards IEEE Std 1012™-2004, IEC 60880:2006 and IEC 61513:2011.
1: FPGA Technology Introduction
2: R&D Achievements
3: Current Research Direction
Current Research Direction

Problems and Challenge

• **How to Use SRAM-FPGA**
  - Advantage for SRAM FPGA (New technology, Large Gates, Additional Choice)

• **Friendly and convenient user interface**
  - Write VHDL codes by User (high requirement for User)

• **Human-System Interfaces**
  - CPU Based and operational system (Product Lifecycle and Price)

• **NuPAC Platform Size, Price and Power Consumption**
  - Two FPGA for each card (High Price and High Power Consumption)
  - Physical Size Limitation (9U card and 350mm Depth)
  - Can’t take advantage of Configuration flexibility in large I&C systems (CAP1400)
Current Research Direction

Partial reconfiguration Technology

Xilinx SRAM FPGA architecture support reconfiguration via internal and external configuration ports, and they also offer a great deal of flexibility in how designs get mapped to the architecture. These devices feature a “non-glitching” technology where, even as the functionality of one part of the user design is reconfigured, static portions of the design—especially routing resources—can overlap this reconfigurable region and not be affected by the act of reconfiguration itself.

We can use this feature to migrate from SEU!

Success in Aerospace Application!
Current Research Direction

- CPLD (Tradition Architecture or Soft-error detected or recover)
- Flash-FPGA
- Anti-Fuse
- ASCI (Application Specific Integrated Circuit)
Current Research Direction

Configuration Software:

• User Logic (For Application)
• Communication Path

Technical Route

• Transition high-level language (e.g. C++, Java) to Hardware Language (e.g. VHLD, Verilog) - Mentor Graphic - Catapult® High-Level Synthesis

• **Develop functional Modules (e.g. 4 too2 Module, Filter Module and etc.) and Configured by SAMA.**

• Develop functional Modules (e.g. 2 too1 Module, Filter Module and etc.) and Configured by Programming Language.
Current Research Direction

Configuration Software (SAMA) Example:
Current Research Direction

How to Verify the Configuration Software

- Qualified the Configuration Software Tool
- Verification & Validation of the Configuration Software Tool Output Result
Current Research Direction

FPGA Based Human-System Interfaces Prototype

- One chip (SRAM Based FPGA)
- No intellectual property (IP), No Microprocessor embedded, No Operation System
- Typical Picture for Human-System Interfaces of CAP1400
Current Research Direction

New Platform (Size, Cost and Power Consumption reduced)

Balance between Traditional PLC/DCS and NuPAC Platform

Group Module(4) Vs One GLM
12 Channel Vs 8 Channel for One card
Two Kind Logic mezzanine
  • For Communication and Logic Process- Two FPGA
  • For I/O Control- One FPGA
## Current Research Direction

### New Platform (NuPAC 200)

<table>
<thead>
<tr>
<th></th>
<th>M</th>
<th>I</th>
<th>I</th>
<th>I</th>
<th>P</th>
<th>O</th>
<th>O</th>
<th>O</th>
<th>U</th>
<th>U</th>
<th>U</th>
<th>U</th>
</tr>
</thead>
</table>

144 I/O Channels

### Current Platform (NuPAC)

<table>
<thead>
<tr>
<th></th>
<th>G</th>
<th>G</th>
<th>G</th>
<th>G</th>
<th>G</th>
<th>G</th>
<th>G</th>
<th>G</th>
<th>L</th>
<th>L</th>
<th>L</th>
<th>L</th>
</tr>
</thead>
</table>

128 I/O Channels

VS

<table>
<thead>
<tr>
<th></th>
<th>C</th>
<th>C</th>
<th>C</th>
<th>C</th>
</tr>
</thead>
</table>

### Additional 2 Cards for communication

<table>
<thead>
<tr>
<th></th>
<th>M</th>
<th>M</th>
<th>M</th>
<th>M</th>
</tr>
</thead>
</table>

©SPIC 2018. All Rights Reserved.
Current Research Direction

New Platform (Size, Cost and Power Consumption reduced)

• 15U Special Chassis Vs 6 U Standard Chassis with Reinforce;
• Depth 458mm Vs 330mm;
• 70 lbs Vs 20 lbs;
谢谢！
THANK YOU！