NNR Regulatory Position on FPGA Based Digital I&C Systems

Gerard Lekhema

National Nuclear Regulator - South Africa

For the protection of persons, property and the environment against nuclear damage.

11th International Workshop on Application of FPGAs in Nuclear Power Plants

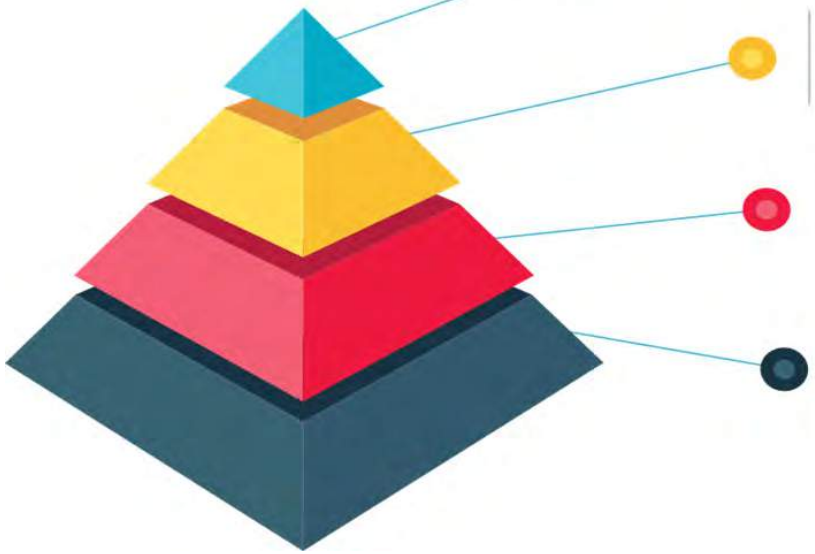
8 – 11 October 2018, Dallas, Texas, USA

Contents

Introduction

- The NPP Regulated by NNR - Koeberg
  - 2 Units each rated at: 921 MW_e (net)
  - Commercial operation since 1984 & 1985
  - Analogue I&C Safety Systems (i.e. RPS)
  - Digital I&C safety related systems (i.e. Reactivity control)
- Expected Digital I&C for Safety Systems:
  - Upgrades and Modifications – Koeberg Plans to extend operating License by another 20 years (Ageing Management and long-term operation)
  - New build – Shelved beyond 2030 as per draft IRP-2018 (Nuclear site license application ongoing)

Regulatory Framework



Level 0

NNR Act, Regulations

Level 1

Regulatory Requirements, Regulatory Directives and Policies

Level 2

Regulatory Guides, Position Papers **

Level 3

Technical Reports (review and research reports) Compliance Assurance Reports (Inspections, audit and Surveillance reports), Safety Evaluation Reports, Letters

** PP-0017: Design and Implementation of Digital I&C for Nuclear Installations - 2014

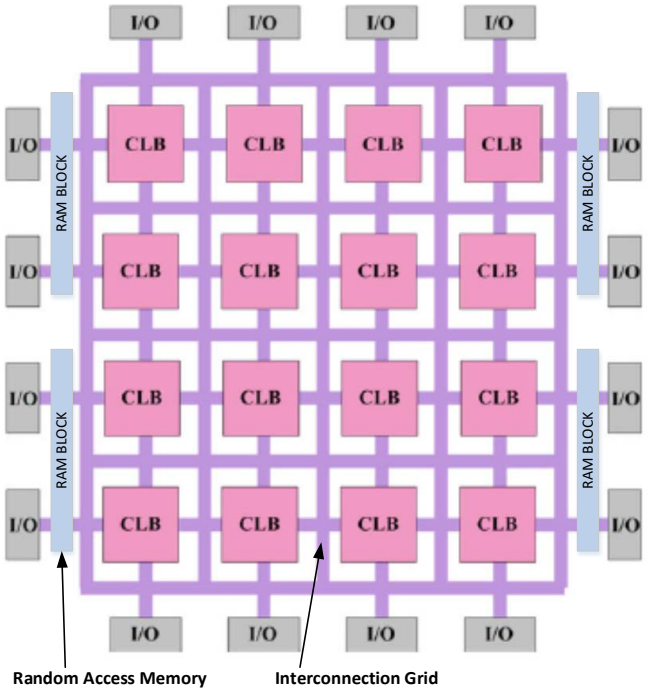
** RG-0014: Guidance on Implementation of Cyber or Computer Security for Nuclear Facilities - 2015

FPGA Based Digital I&C Systems

- Some of the upgrades and new build are expected to be fitted with digital I&C for Systems important to Safety.
- Weaknesses of software-based systems (i.e. PLCs, DCS): complexity, credible common cause failures, etc.
- Increasing trend in use of FPGA based systems.
- NNR participates in information sharing platforms (MDEP DICWG, Conferences, etc.) and references international standards and guides, in preparation for anticipated FPGA based digital I&C modifications/new builds.

FPGA Architecture

- FPGA is a hardware description language programmable integrated circuit comprised of:
  - Configurable logic blocks (CLB)
  - Programmable input/output (I/O)
  - Programmable interconnection grid
  - Application data memory



FPGA Advantages and Challenges

Advantages	Challenges
Lower Complexity, simpler V&V, faster response time, module-for-module replacement	Relatively few NPP applications with limited operating experience
Parallel Processing Capabilities	Limited availability of products and tools
Reduced vulnerability to cybersecurity threats	Specialized design expertise required
Longer availability of technical support	Development process similar to software-based systems and thus subject to same logic errors
Less prone to obsolescence due to greater application portability	Increasing complexity with IP cores results in 100% testing difficult to achieve

Addressing FPGA Challenges

- Simplicity in design – only features beneficial to safety should be included.
- Application of diversity and defense-in-depth for protection against credible common cause failures
- Standardized development life-cycle and quality assurance plan (i.e. IEC 62566): Requirements specifications, preliminary design, design, implementation, system integration and system validation

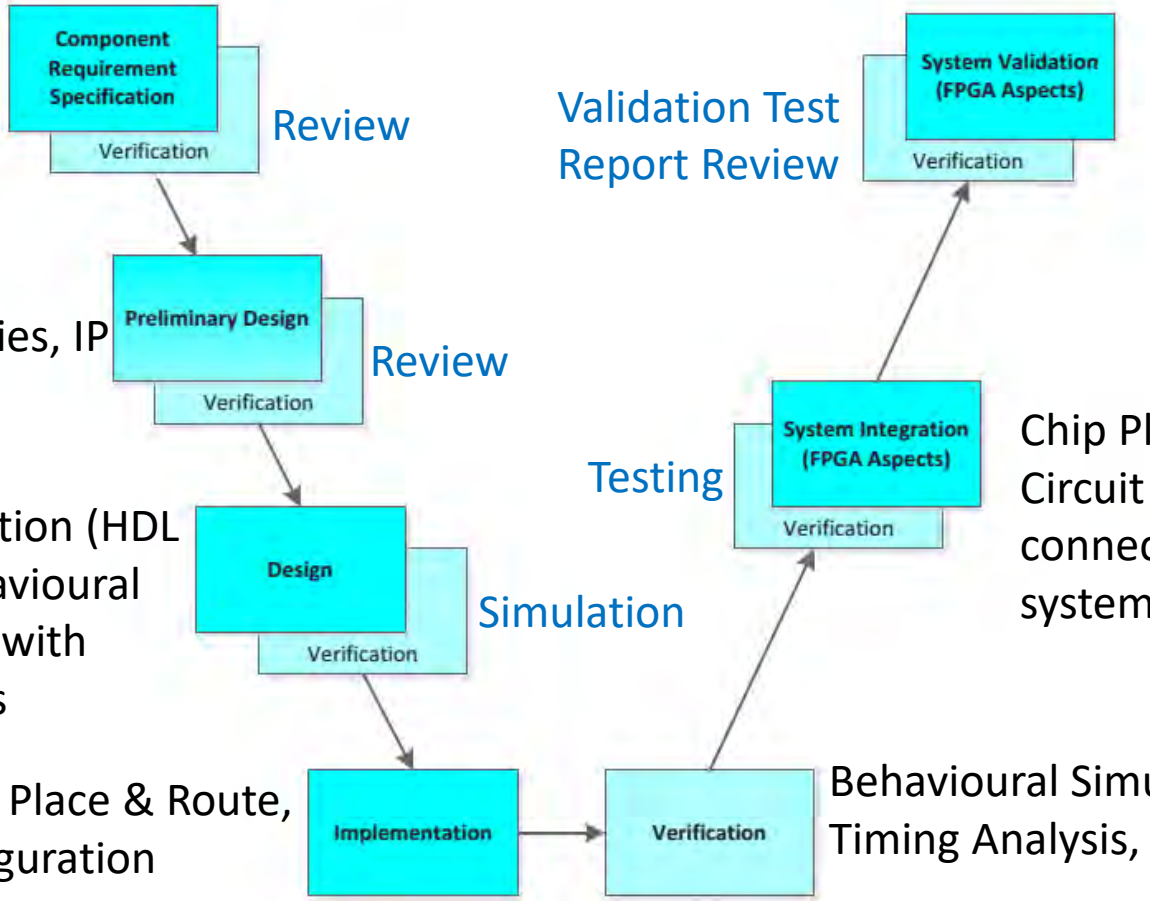
FPGA Development Life-Cycle

Final Product Properties: Functional, etc.

Architecture: Modules, Libraries, IP Cores, etc.

RTL Description (HDL Code): Behavioural description with coding rules

Synthesis, Place & Route, chip configuration



Evaluation of compliance with requirements

Chip Placement on Circuit Board and connections to other system components

Behavioural Simulation, Timing Analysis, Testing

*IEC 62566, IAEA NP-T-3.17, SSG-39

NNR Regulatory Position

- NNR Position is derived from the generic position paper PP-0017 on digital I&C systems and reg. guide RG-0014 on cyber security.
- The FPGA based digital I&C system is suitable for important to safety application. NNR strongly prefers hardware-based backup system in order to fulfil diversity and defense-in-depth requirements for protection against common cause failures.
- The FPGA system should be developed under a nuclear safety and quality management program that addresses the entire life-cycle of the FPGA system.
- The pre-developed/commercial-grade items (i.e. IP cores, software tools, application memories, etc.) should undergo an approved nuclear quality assurance program.

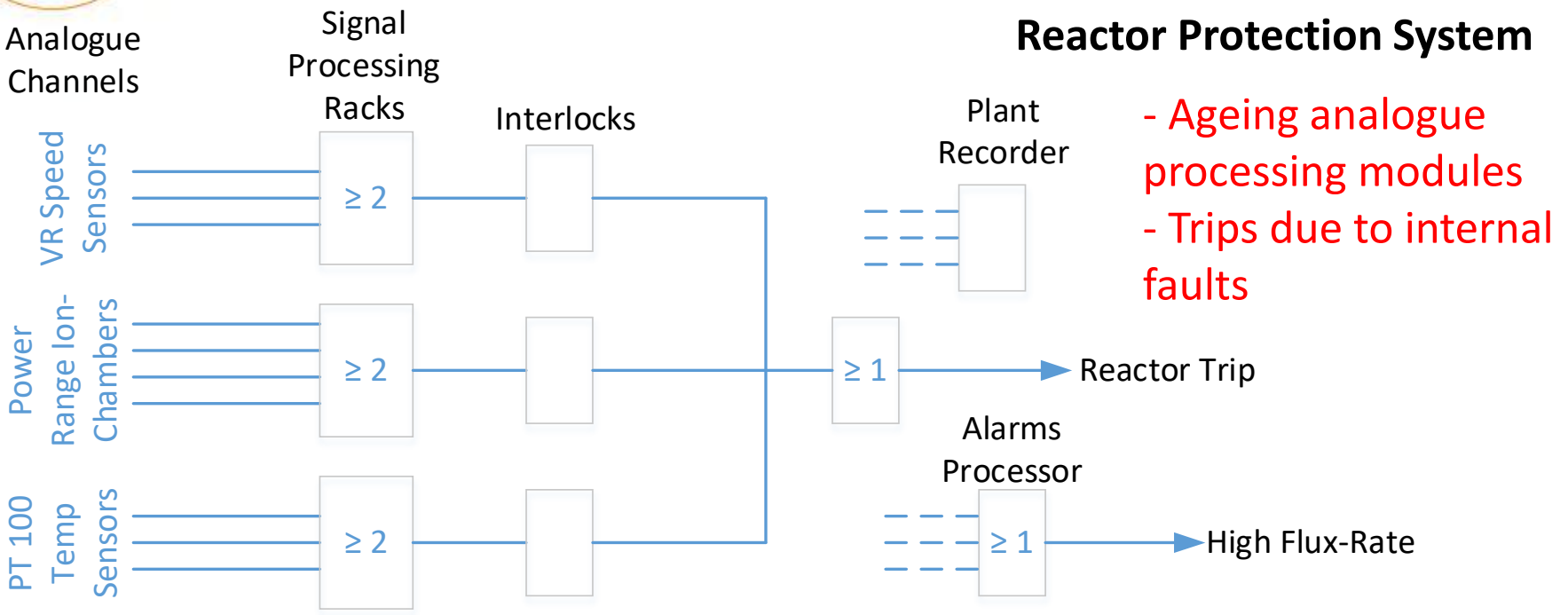
NNR Regulatory Position…cont.

- The use of FPGA with Intellectual Property (IP) cores in important-to-safety applications should be avoided to prevent unnecessary complexity.

- Reference standards and guides: IEC 62566, IEEE 7-4.3.2-2010, IAEA SSG-39, IEC 60880, IEC 60987

- The less prescriptive regulatory approach of NNR specifies that the authorization holder/applicant should compile a safety case using best suited standards that represent good engineering practice. The NNR makes determination as to whether the justification is adequate.

Example of FPGA Based Application



- FPGA Based Passive Speed Sensors Processing modules
- Reliability Improvement, self-diagnostic features

Conclusion

- The FPGA based digital I&C system is simpler compared with microprocessor-based system.

- Experience and information from the progressive FPGA based modernization/new build projects will assist NNR in making regulatory decision for anticipated FPGA based projects in South Africa.

THANK YOU

Gerard Ratoka Lekhema
Analyst - NPP Assessments Department

National Nuclear Regulator – South Africa
Phone: +27 (12) 674 7157
Mobile: +27 (83) 667 2138
Email: glekhema@nnr.co.za

Eco Glade Office Park I Eco Glades Office 2 Block GI 420 Witch Hazel Avenue I Centurion
P. O. Box 7106 I Centurion I 0046 I South Africa