9th Workshop on the Application of FPGAs in NPPs

Principles for FPGA based I&C platform redesign and class 2 qualification

EDF
Research and Development, Instrumentation and Control (R&D)
Frédéric Daumas (frederic.daumas@edf.fr)
Engineering Support, Dismantling and Environmental Services Division, Nuclear Island Engineering (DIPDE)
Michel Agremont (michel.agremont@edf.fr)
Nuclear Engineering Division, Basic Design (SEPTEN)
Alexander Wigg (alexander-john.wigg@edf.fr)

GE
Industrial Solutions, Automation and Controls
Arthur Lefebvre (arthur.lefebvre@power.alstom.com)

Presentation Plan :

1. Context and objective

2. Methodology

3. Main concerns

4. Recommendations

Context

- Past R&D activities have investigated use of FPGA technology for safety systems
  - MC6800 emulator development and formal verification with RRCN
  - Supporting IEC SC45A WGA3 “Instrumentation and control important to safety” normalization work ➔ IEC 62566 (2012)

- Current partial system renovation projects are focused on electronic boards or components replacement (obsolescence treatment) using HDL -Programmable Devices (HPDs) technology (e.g. FPGA and CPLD integrated circuits)

- IEC/SC45A - 2016 ROK meeting : proposal to develop a standard establishing requirements for
  - *"Development of HDL-programmed integrated circuits for systems performing category B or C functions"*

Supporting case study and objectives

- GE is performing for EDF a redesign of one CONTROBLOC electronic module using FPGA technology
  - Limited variability language PLC platform in charge of logic I&C functions for 1300MW NPPs
- The main objectives:
  - Assess the ability to qualify such redesign project towards safety class 2 requirements (IEC 61513)

    ➔ Assess feasibility to build a justification case for class 2 I&C system FPGA based development following proven industrial practices positioned towards requirements applicable to category A functions HDL-programmed lifecycle (specification, design, implementation, V&V, modification, …)

  - Provide inputs for the IEC/SC45A WGA3 «Application of digital processors to safety in nuclear power plants» normalization work

    ➔ New project draft (NWIP) dealing with the use of Hardware Description Language (HDL)-Programmed Devices (HPD) for systems performing category B and C functions

Methodology for the case study 1

- Development of the re-designed module is based on a suitable set of requirements which are derived from IEC 62566 and based on engineering judgment, analysis and rational negotiation with the supplier

  - As a first task of the Qualification Plan for class 2, GE / ALSTOM carried out a detailed evaluation of the applicability of main I&C standards such as IEC 61513, 62566, 60880 and 60987

  - Technical discussions between GE and EDF (DIPDE, SEPTEN and R&D) focused on IEC 62566 requirements to reach a consensus about the subset of requirements that have to be fulfilled for this development

  - Discussions with ASN technical support organization (IRSN) to validate interpretation on a selection of issues

Methodology for the case study 2

- Scope of the detailed review

  - ~400 requirements and recommandations from IEC 62566 (clauses 5 to 17)
    - references to common points with software development (IEC 60880)
    - references to system issues (IEC 61513)
  - 140 more items from IEC 60880 (Ed.2) normative annexes A and B where “HPD” substitutes to “software”

- Classification principle
  - Conformance for class 2 qualification (with interpretation)

    ➔ refer to acceptable practices for cat. B software development (IEC 62138)

  - Not applicable (with justification)

  - Not relevant (with project related justification)

Some issues discussed

- Self-monitoring and fault tolerance
- Use of tools (development, configuration management, V&V)
- Requirement for determinism ➔ Predictability of system behavior
- FMEA and reliability justification
  - separation between safety classified and non-safety parts (sub-functions and modules)
- Documentation of the tools and FPGA selection and acceptance processes
- Simulation (RTL, Post Place and Route)
  - acceleration techniques and « key point » tests to run
- Coverage rates (quantified objectives)
- Development steps documentation and requirements traceability

Recommendations

- This case study constitutes an example of application of IEC 62566 requirements by an experienced developer of industrial nuclear safety systems familiar with standards dealing with I&C systems important to safety in the nuclear field (IEC 61513) and in the functional safety domain (IEC 61508)
  - This case study demonstrates the need for graduation
  - Input to future standard regarding use of HPD development for category B and C I&C applications
- The application of a new standard to an existing legacy system limits the relevance of the standard and may reduce its potential applicability to other projects
- There is a need to make the future standard document IEC 62566-2 more freestanding (within IEC editorial constraints)
- It would be valuable to provide as many relevant examples as possible to guide future standard IEC 62566-2 application and assessment

Thank you for your attention.

Frédéric Daumas (frederic.daumas@edf.fr)
Alexander Wigg (alexander-john.wigg@edf.fr)