NewClear Day Inc.

9th International Workshop on
the Application of FPGAs in NPPs
Lyon, France

NRC Topical Report Certification Process: *Suggestions for Success*

Mark Burzynski

October 5, 2016

Purpose

Provide suggestions for successful NRC review and approval of an FPGA-based topical report

- FPGA Platform Review Scope
- NRC Software-Based Regulatory Guides
- FPGA Development Tools
- Secure Development and Operating Environments
- Equipment Qualification
- Self-Testing Features

FPGA Platform Review Scope (1/3)

A topical report should focus on:

- Hardware design, qualification, and analysis
- Generic programmable logic and associated development life cycle processes (which includes application-oriented library of re-usable programmable logic components)
- Toolset used to design and implement the system architecture, configure the units and networks, and develop the project-specific programmable logic
- Project-specific development life cycle processes

NewClear Day Inc.

FPGA Platform Review Scope (2/3)

A topical report should also address platform interfaces:

- Input connections to field devices but not the field devices
- Output connections to field devices but not the field devices
- Keyswitch interfaces for keyswitch inputs that support platform access control features used to support system maintenance activities but not the keyswitch design or location
- Platform communication independence features that support interfaces for export of data to an online monitoring system or a plant computer system but not the online monitoring system hardware or software

FPGA Platform Review Scope (3/3)

A topical report should also address platform interfaces:

- Platform communication independence and data transfer protocol features that support communication with a maintenance workstation to adjust setpoints and other predefined calibration factors but not the maintenance workstation
- Module connections and data protocols for loading electronic design configuration files but not any download station

NewClear Day Inc.

Use of IEC Standards

NRC is now more accepting of international standards, especially where IEEE Standards are silent regarding FPGAs

- Need to describe relevance and use of international standards such as:
  - IEC 62566:2011
  - IEC 61508:2010
  - IEC 60987:2013
  - IEC 60880:2006
  - IEC 61513:2001

NRC Software-Based Guidance (1/6)

Regulatory Guide (RG) 1.168, Revisions 2, endorses IEEE Std 1012-2004 structured approach to software V&V

- V&V programs activities and tasks need to be adapted to reflect important process differences and exceptions
  - V&V Activities adapted to company development life cycle and FPGA technology
    - Need to have a clear strategy on when electronic design ends (i.e., linkage with module hardware development) in defining activities
  - V&V Tasks adapted to FPGA technology
    - Need to be clear on FPGA-specific tasks (e.g., logic and timing simulation and static timing analysis) for independent review, verification, and validation

NRC Software-Based Guidance (2/6)

RG 1.168, Revisions 2, endorses IEEE Std 1012-2004 as a structured approach to software V&V

- Exceptions to specific documentation requirement details that conflict with established design practices and quality assurance program requirements
  - Test documentation requirements (Section 6.3.1)
  - Administrative and formatting requirements (Sections 7 and 8)
  - Criticality analysis should not be necessary, since FPGA electronic designs are required to be classified at highest level for use in safety systems
  - FMEDA should replace hazards analysis (Section 5 and Tables 1 and 2)
  - Security vulnerability assessments performed for RG 1.152, Revision 3, should replace security analyses (Section 5 and Tables 1 and 2)

NRC Software-Based Guidance (3/6)

RG 1.168, Revisions 2, endorses IEEE Std 1028-2008 as an acceptable method to perform software reviews and audits

- Standard does not define what reviews and audits should be performed
- Need to define required reviews and audits as part of the Software Quality Assurance Plan and specify if any of the activities will follow the administrative and documentation requirements from IEEE Std 1028-2008

NewClear Day Inc.

NRC Software-Based Guidance (4/6)

RG 1.172, Revision 1, endorses IEEE Std 830-1993 for methods to develop software requirements specifications

- Requirements specifications should be tailored to FPGA technology
- Ranking requirements for importance or stability for safety systems is not necessary, since unnecessary requirements should not be imposed in safety systems
- Exceptions to specific documentation requirement details that conflict with established design practices and quality assurance program requirements

NRC Software-Based Guidance (5/6)

RG 1.171, Revision 1, endorses IEEE Std 1008-1987 for unit test requirements

- Unit testing requirements should be tailored to FPGA technology
- Exceptions to specific documentation requirement details that conflict with established testing practices and quality assurance program requirements

NRC Software-Based Guidance (6/6)

RG 1.170, Revision 1, endorses IEEE Std 829-2008 for test documentation requirements

- Test documentation requirements should be tailored to FPGA technology
- Documents can be combined or eliminated, as allowed by the standard
- Exceptions to specific documentation requirement details that conflict with established testing practices and quality assurance program requirements

NewClear Day Inc.

FPGA Development Tools

Various NRC documents provide guidance relevant to FPGA tools:

- DG-1292, *Dedication of Commercial-Grade Items for Use in Nuclear Power Plants*, reinforces existing commercial grade dedication guidance for digital platforms (i.e., EPRI TR-106439 and -107330). EPRI TR-107330 Section 4.4.4 addresses capabilities for software development tools.
- RG 1.152, Revision 3 endorses IEEE Std 7-4.3.2-2003, which specifies requirements for use of software tools in Section 5.3.2.
- Branch Technical Position 7-14 provides some limited guidance on use of software tools (at pages 19 and 20).
- DG-1305, *Acceptance of Commercial-Grade Design and Analysis Computer Programs for Nuclear Power Plants*, makes it clear that endorsed guidance for design analysis tools does not apply to software development tools used for software embedded/installed in plant safety systems.

These NRC guidance documents should be satisfied with tools that satisfy IEC 62566:2012 Sections 8.2, 8.5, and 15

NewClear Day Inc.

FPGA Partitioning

FPGA technology can use partitioning of electronic designs to achieve functional independence

- Need to explain how partitioning is used to achieve functional independence
- Need to explain how partitioning is controlled in design and implementation

NewClear Day Inc.

FPGA Self-Testing Features

FPGA technology can lead to different self-testing features than comparable microprocessor-based systems

- Need to explain operation and coverage of self-testing features
- Need to demonstrate how self-testing performance and test routine integrity are ensured
- Need to show how self-testing and self-monitoring features can be used to replace standard analog system surveillance tests
  - Export of input channel data for automated comparison and alarm in online monitoring system can replace existing analog channel checks
  - Self-testing features can replace standard analog channel functional tests used to verify setpoints and protection systems trip actuation capability (e.g., continuously checking integrity of module electronic design or monitoring FPGA operating with a watchdog timer)
  - Auto-calibration features in input modules can simplify standard channel calibration surveillance requirement for entire instrument loop

FPGA Diversity

FPGA technology can lead to different strategies for use of diversity to minimize or eliminate software common cause failure vulnerabilities

- Need to define diversity strategy and its basis
- Need to establish a clear link between diversity attributes and specific software common cause failure vulnerabilities
- Need to demonstrate how diversity strategy minimizes or eliminates software common cause failure vulnerabilities
- Need to anticipate questions about differences from generic list of diversity attributes and previously approved precedents

Secure Development and Operating Environments

FPGA technology can lead to different technical issues with data flow control and physical access

- Requirements management methods should be sufficient to demonstrate that all necessary functionality is provided and no unwanted functionality has been added during design
- Configuration item control measures should be sufficient to ensure identify and no alteration during implementation
- One-way hardware data flow control implemented within the FPGA for safety to nonsafety interface will need to be shown as robust
- Physical access controls other administrative controls will need to be addressed to configurable FPGA designs (both for tunable parameters and configuration changes)

NewClear Day Inc.

Equipment Qualification

FPGA technology does not present and significant differences for equipment qualification testing; however, there are a few points of emphasis

- Need to determine test levels for electrical tests based on expected service conditions
- Determine scope of magnetic susceptibility testing based on expected equipment location
- Need to adapt EPRI TR-107330 test guidance to reflect platform input and output design features
- Need to adapt EPRI TR-107330 test guidance to reflect qualification test specimen scope (e.g., power supplies included or not)

NewClear Day Inc.

Summary

- Topical report review scope should encompass platform, platform interfaces, and FPGA development process
- Use of applicable regulatory guidance requires thoughtful tailoring and practical exceptions for FPGA technology
- Certain technical features warrant special attention to derive full benefits from FPGA use

> ***There are no secrets to success. It is the result of preparation, hard work, and learning from failure.***
>
> *Colin Powell*