U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Licensing Field-Programmable Gate Arrays in Safety Systems

Bernard F. Dittman, Electronics Engineer (Digital I&C)
Instrumentation and Controls Branch (EICB)

Prepared for the
IAEA co-sponsored 3rd Annual Workshop on the
Application of Field-Programmable Gate Arrays (FPGAs) in Nuclear Power Plants

September 28 – October 1, 2010
Hamilton, Ontario Canada

The information and conclusions presented herein are those of the author only and do not necessarily represent the views or positions of the U.S. Nuclear Regulatory Commission. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use of this information.

Licensing FPGAs in Safety Systems

- Overview
  - Summarize the Wolf Creek licensing experience
  - Summarize subsequent licensing experiences
  - Discuss the limitation of the Wolf Creek safety evaluation
  - Discuss coordination and mapping Digital Instrumentation & Control (DI&C) Interim Staff Guidance (ISG) #6, "Licensing Process," information between a safety system platform topical report submittals and each license amendment request that references the platform.
- Digital I&C Interim Staff Guidance #6, is found at:

  http://adamswebsearch.nrc.gov/idmws/ViewDocByAccession.asp?AccessionNumber=ML101800172

Summary of Wolf Creek Licensing Experience

- Wolf Creek's Main Steam and Feedwater Isolation System upgrade – License Amendment Request, March 14, 2007 (ML070800193)
  - Uses a FPGA-based platform
  - Performs the portion of the containment isolation function that responds to automatic and manual command signals to provide actuation signals to isolation valves
  - Involved building a consensus that the design and development of programmable hardware logic-based systems should be reviewed against the applicable regulatory evaluation criteria currently in place for microprocessor software-based systems.

Summary of Wolf Creek Licensing Experience

- The NRC Staff Safety Evaluation Report - March 31, 2009 (ML090610317)
  - Contains a review against the 10 CFR 50.55a (h)(3) incorporated by reference standard, IEEE Std. 603-1991 "Criteria for Safety Systems for Nuclear Power Generating Stations"
  - Applies regulatory evaluation criteria of NUREG-800, Standard Review Plan (SRP), Chapter 7, to establish a precedent for information submittals for FPGA-based programmable safety systems
  - Supplements SRP guidance with Digital I&C Interim Staff Guidance
  - Contains a "*limited*" approval of the methods used and the resultant built-in diversity
- The presentation made at the 2nd Annual FPGA Workshop in Kirovograd, Ukraine provided important considerations to take away from the Wolf Creek licensing experience.

Subsequent FPGA Licensing Experiences

- Use of "Topical Report Process" (LIC-500) pre-submittal meetings
  - Provide an opportunity for early exchanges with the NRC staff, requests for clarifying information, and documented staff feedback regarding topical report contents.
- These pre-submittal (Phase 0) meetings have
  - Provided information to applicants about the staff's evaluation criteria that will be applied to software programmable hardware logic devices, like FPGAs
  - Documented Staff feedback on proposed approaches to build design diversity into safety system platforms, if used.
  - Encouraged a complete mapping of the Digital Instrumentation & Control (DI&C) Interim Staff Guidance (ISG) #6, "Licensing Process," between the platform topical report submittal information and application-specific license amendment request information.

Subsequent FPGA Licensing Experiences

- Phase 0 meetings have also included discussions of platform topical report content that, if provided, would improve follow-on license amendment request safety evaluations, including:
  - Specific examples that demonstrate the correct use of each platform feature
  - The underlying setpoint calculation error term data and basis to support licensee setpoint calculations and determinations of equipment degraded operability
  - Approaches for limiting the time that a division, train or channel may be left in bypass mode, and the means by which equipment inoperability or degraded operability will be determined
  - Identification of required licensee actions to form a starting point for the safety evaluation's plant specific action items

The Limitation of Wolf Creek's Approval

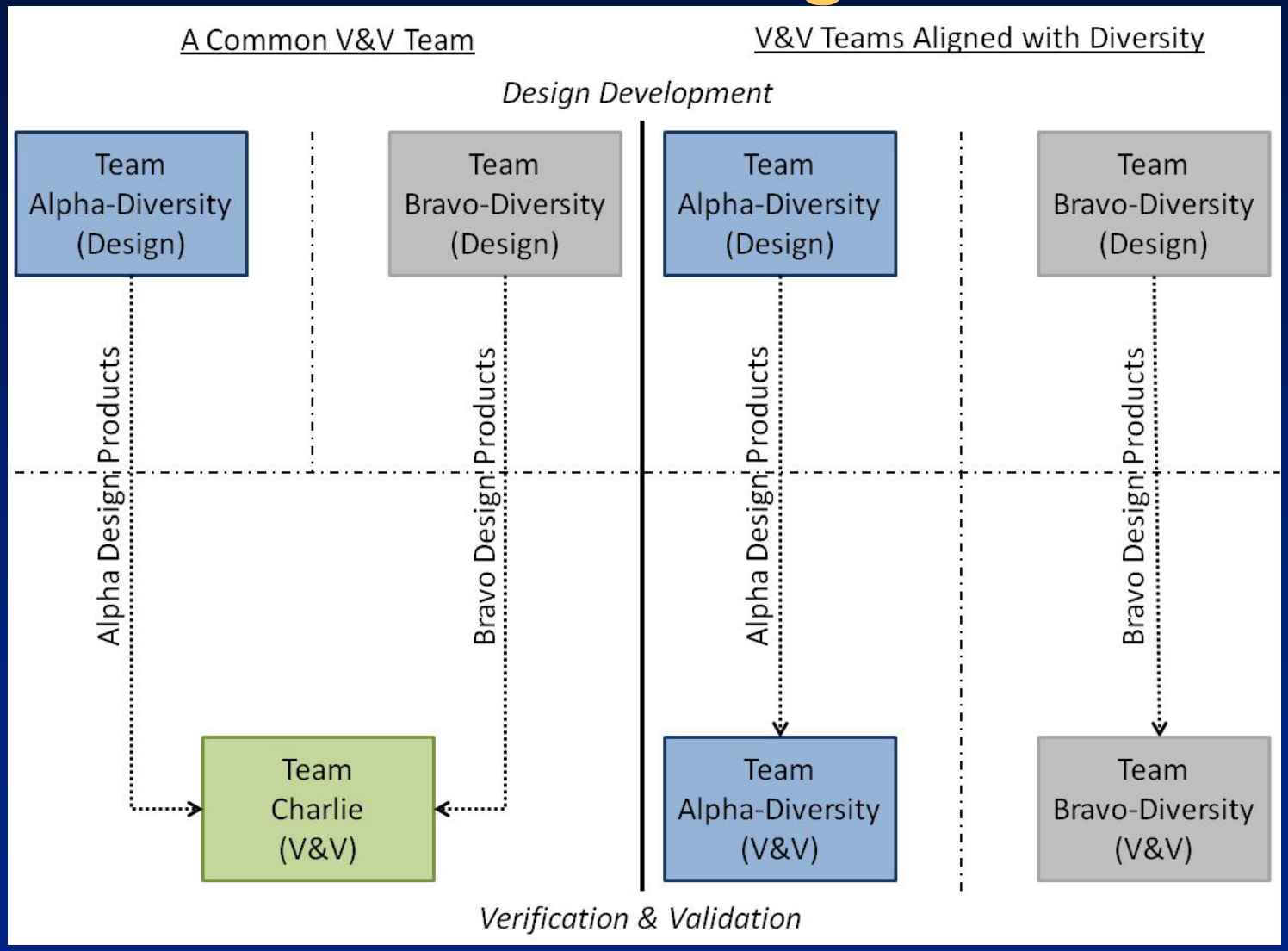
- The safety evaluation's limitation applies to the application-specific and mostly proprietary approaches taken to:
  - Build design diversity into the platform sufficient for the functionality performed by the Main Steam and Feedwater Isolation System
  - Meet regulatory evaluation criteria within documented processes
  - Address implementation specific failure modes and effects
  - Demonstrate adequate plant-specific diversity and defense-in-depth
  - Perform verification & validation on the platform and application.
- The safety evaluation states that the specific methods and resultant degree of built-in design diversity of an FPGA-based platform for an application like the Main Steam and Feedwater Isolation System should be augmented in future applications of greater complexity or safety significance to provide an equivalent degree of assurance.

Addressing the Approval Limitation

- Pre-submittal licensing discussions between the NRC staff and FPGA-based platform applicants have taken a broader aim at systematically eliminating programming errors as a source of common-cause failures through platform diversity attributes and the high quality design process used in the platform's development.

- These pre-submittal licensing meetings have included discussions of:
  - Team configurations (requirements, design, V&V, and quality assurance) to ensure a sufficiently diverse design is produced in the platform and its subsequent applications
    - Team alignments with intended built-in diversity
    - Team independence, as supported by organizational structure

Possible Team Alignments



Addressing the Approval Limitation

- The pre-submittal licensing meetings have also included discussions of ways to enhance built-in diversity to provide greater safety assurance for the targeted level of safety significance or equipment complexity.
- Approaches to embed diversity at the FPGA platform level include use of different:
  - FPGA programming techniques or specification languages
  - Logic synthesis directives
  - FPGA devices
  - Implementation teams (as shown previously)
  - Platform algorithms
- Approaches to provide diversity at the application level include:
  - Multiple diverse implementations within a redundant channel or segregating diverse implementations to mutually exclusive channels
  - Diversity through specification or use of a formal diversity judge/arbitrator

Use of DI&C Interim Staff Guidance #6

- Pre-submittal licensing discussions between the NRC staff and FPGA-based platform applicants have applied the content and phased submittal information defined in the DI&C-ISG-06, “Licensing Process.”
- The associated platform topical reports are mapping DI&C-ISG-06 safety evaluation review information, as appropriate, among various content, as follows:
  - The platform topical report submittal
  - An application-specific platform submittal
  - The license amendment request submittal
- Following the review of the platform topical report and a digital I&C license amendment request that references it, this approach will ensure that a complete set of information has been made available to the NRC staff and evaluated before a plant-specific application of an FPGA platform is placed into service.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Conclusions

- Wolf Creek's licensing experience provides a foundation for evaluating applications of the FPGA technology when addressing equipment obsolescence.
- Nevertheless, the scope and limitations of this approval must be understood in the context of complexity and potential sources of programmable device common-cause failures.
- This understanding is needed to produce sufficient built-in diversity that is adequately documented in the platform's design basis to enable a deterministic evaluation of common-cause failure sources and the plant's ability to cope with any remaining vulnerability.
- Both an IEEE Standard specifically targeting the FPGA technology's use in nuclear power plants, and industry guidance to map applicable DI&C-ISG-06 Enclosure B information for FPGA-based platforms could:
  - Further improve regulatory review efficiency and consistency
  - Benefit the nuclear power industry by creating a broader and more consistent industrywide consensus while eliminating some drawbacks of proprietary information protection.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Questions & Discussion