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

Case Study for Tailoring and Adapting IEEE Std 1012 Software Verification and Validation Requirements for FPGA Technology

Mark Burzynski
Chief Executive Officer

October 8-11, 2018
Dallas, Texas, USA

Sunport
Connecting Forward

Reason for Case Study

- Key challenge for review of FPGA-based I&C systems in the US is use of IEEE Std 1012-2004, which is endorsed in NRC Regulatory Guide 1.168, to develop appropriate software V&V plan
- V&V tasks defined in IEEE Std 1012 are based on a software-centric development model
- An FPGA-centric development model has important differences for electronic design and implementation tasks
- Use of IEEE Std 1012 to define V&V requirements for FPGA-based I&C applications will always require standard requirements to be tailored and adapted to FPGA technology

Outline for Case Study

- A case study is presented that identifies the tailoring and adaptations necessary for a digital I&C platform developed to IEC standards for systems performing Category A functions
- The following topics are assessed:
  - Development Life Cycles
  - Definition of Required V&V Tasks
    - General Analysis Tasks
    - Specific Verification Tasks
  - Development Tools
  - V&V Independence
  - Documentation

Development Life Cycles (1/2)

- IEEE Std 1012 framework is based on a specific development life cycle process
  - Allows for adapting development process and tailoring minimum task requirements for specific software development methods and technologies (e.g., automated code generation from detailed design) that may eliminate development steps or combine several development steps into one
- IEC development life cycle is an integrated approach that starts with the system level (in IEC 61513) and flows down to hardware and software allocations (in IEC 60987 and IEC 60880)
  - IEC 62566 is a second level document that focuses on the activities when Hardware Description Language (HDL)-Programmed Devices (HPDs) are developed

Development Life Cycles (2/2)

IEEE Std 1012	IEC 61513	IEC 62566
Concept	System safety and architecture concept	
Requirements	System requirements specification	HPD requirements specification
	Suitability analysis	
Design	System detailed design	HPD design
Implementation	System implementation	HPD implementation
	System integration	HPD aspects of system integration
Test	System validation	HPD aspects of system validation
Installation and checkout	System installation and commissioning	

- Development lifecycle for HPDs can be adapted based on IEC 62566 development life cycle, as allowed by IEEE Std 1012

Definition of Required V&V Tasks

- IEEE Std 1012 defines minimum V&V tasks required for different software integrity levels (SIL) and specifies development phase where V&V tasks are to be performed
- IEC 62566 provides more comprehensive requirements for the verification process, which are tightly bonded with the verification object
  - IEC 62566 has flexibility on when V&V tasks are performed
  - Additional tailoring of IEEE Std 1012 requirements related to when V&V tasks are performed is required to retain the flexibility allowed by IEC 62566
- IEEE Std 1012 V&V tasks for SIL 4 fall into two categories that warrant further discussion: general analysis tasks and specific verification tasks.

General Analysis Tasks (1/4)

- General analysis tasks are specified for each development phase and initial analysis is to be updated in subsequent phases
- Criticality Analysis task is intended to assign a SIL to a software component based on a pre-defined risk-based classification scheme
  - NRC specifies SIL 4 for safety-related software
  - IEC 62566 is written specifically for Category A functions

Criticality Analysis tasks have no value for nuclear safety-related systems and an exception to the IEEE Std 1012 requirements is needed to eliminate them

General Analysis Tasks (2/4)

- Hazard Analysis task is intended to 1) identify potential system hazards, 2) assess severity, 3) assess probability, and 4) identify mitigation strategies
- IEEE Std 1012 guidance not developed for nuclear industry
  - Approach to hazards is more general, which requires interpretation to understand scope and depth for analysis
- The IEC 62566 guidance is supportive of upper tier guidance in IEC 61513 and 60880 and addresses hazards in three ways:
  - Specific system requirements based on plant safety analysis
  - Specific technology requirements to ensure deterministic behavior of the digital equipment
  - Requirements to minimize human errors during system development and operation
- Hazards for a digital I&C platform may be documented in an FMECA or FMEDA

General Analysis Tasks (3/4)

- Security Analysis task is intended to 1) review an acceptable level of security risk and 2) analyze system design features that mitigate identified vulnerabilities associated with the environment and system interfaces
- IEEE Std 1012 guidance is not specifically developed for the nuclear industry
  - Approach to security is general and V&V tasks are redundant to security analyses performed by others to satisfy RG 1.152 and RG 5.71 requirements
- IEC 62566 guidance is supportive of upper tier guidance in IEC 61513 for system security plan and specifies that software security requirements specified in IEC 60880 apply to development of HPDs
- An exception to the IEEE Std 1012 requirements is required to eliminate redundant tasks

General Analysis Tasks (4/4)

- Risk Analysis task is intended to 1) identify technical and management risks and 2) provide recommendations to eliminate, reduce, or mitigate risks
- IEEE Std 1012 guidance is not specifically developed for nuclear industry and approach to project risk management is general
  - RG 1.152 endorses IEEE Std 7-4.3.2, which also addresses project management risk more comprehensively than IEEE Std 1012
- IEC 61513, 60880, and IEC 62566 address technical and human error risks; however, they do not explicitly address project management risk
- Additional Risk Analysis tasks must be performed to satisfy IEEE St 1012, and IEEE Std 7-4.3.2
  - An exception to IEEE Std 1012 requirements may be required to eliminate redundant tasks if project risks are evaluated as part of the project management process

Specific Verification and Validation Tasks (1/5)

- **Specific V&V tasks in IEEE Std 1012 are organized by development phase, as shown in a set of tables**
- **IEC 61513, IEC 60880, and IEC 62566 collectively address the following tasks in a manner comparable to IEEE Std 1012:**
  - **Concept documentation evaluation**
  - **Hardware/software/user requirements allocation analysis**
  - **Software requirements evaluation**
  - **Software design evaluation**
  - **Source code and source code documentation evaluation**
  - **Interface analysis**
  - **Traceability analysis**
  - **Installation checkout**
  - **V&V final report generation**

Specific Verification and Validation Tasks (2/5)

- IEC 62566 specifies that output of each development phase shall be verified
  - This approach allows for direct use of vendor tools to produce standard design outputs that are then verified
- IEC 62566 provides additional guidance relevant to HPDs for systems performing Category A functions:
  - Verification of the use of the pre-developed items
  - Verification of the RTL design and implementation
  - Static verification (equivalent to source code evaluation)
  - HPD aspects of the system integration
  - HPD aspects of the system validation
  - HPD aspects of installation, commissioning and operation

Specific Verification and Validation Tasks (3/5)

- IEEE Std 1012 defines testing requirements from a software perspective
  - Component V&V testing
  - Integration V&V testing
  - System V&V testing
  - Acceptance V&V testing
- IEC approach defines testing requirements with an integrated approach encompassing the full system, including hardware, software, and HPD
- IEC integration, system, and acceptance validation testing requirements for software and HPD are consistent with the IEEE Std 1012 requirements

Specific Verification and Validation Tasks (4/5)

- HPD technology electronic designs for target hardware cannot function in isolation from hardware, so stage-wise integration testing is not possible
- Behavior modeling (i.e., HDL only) can be performed to a certain extent; however, complete modules have to be used for testing
- Modules of typical digital I&C platforms cannot function in isolation, so only minimal “module component” tests can be done without integrating the platform system
- As a consequence, more requirement tracings for HPD technology systems that ensure that every requirement is tested terminate at hardware/system integration testing than is typical for microprocessor/software technology

Specific Verification and Validation Tasks (5/5)

- IEC 62566 electronic design verification testing requirements are tailored for HPD technology and are different than IEEE Std 1012 Component V&V testing requirements
- HPD technology relies on simulation models and test benches to evaluate the behavior and performance characteristics during the HPD design and implementation development phases
  - Testing is required following on Register Transfer Level descriptions (design phase) in order to confirm correctness
  - Testing is required to confirm that Post Route descriptions (implementation phase) complies with timing constraints, including back-annotations
  - Simulation tests (i.e., static timing analyses) are performed using simulation for both “worst case” and “best case” to ensure deterministic behavior

Other V&V Program Requirements (1/2)

- IEEE Std 1012 has limited requirements associated with software development tools
  - RG 1.168 modifies the IEEE Std 1012 guidance by specifying IEEE Std 7-4.3.2, which requires either a test tool validation program or that software tools be used in a manner such that defects not detected by the software tool will be detected by V&V activities
- IEC 60880 and IEC 62566 have an extensive set of requirements that address the selection, qualification, configuration management, and use of software development tools and the automation of testing to reduce human errors
- IEC 62566 addresses V&V organizational independence in a manner comparable to RG 1.168

Other V&V Program Requirements (2/2)

- IEEE Std 1012 specifies a prescriptive format, including topics, order, and content for the V&V plan document
- IEEE Std 1012 outlines required testing tasks and documentation based on prescriptive and extensive documentation requirements specified in IEEE Std 829
- IEC standards are less prescriptive about V&V plan and test documentation structure and format
- A deviation to the IEEE Std 1012 requirements is required to use an alternate V&V plan and test documentation structures and formats

Sunport
Connecting Forward

www.sunport.ch

Thank you

SunPort SA

LaCite Business Nucleus Avenue
De l’Universite 24 CH-1005
Lausanne, Switzerland
t: +41 213 123 901