Using IEEE 1012 for V&V of FPGA-Based Equipment: Perspectives from the IEEE P1012 Working Group

David Hooten

12th International Workshop on Application of Field Programmable Gate Arrays in Nuclear Power Plants

14 October 2019

FPGA Workshop Interests

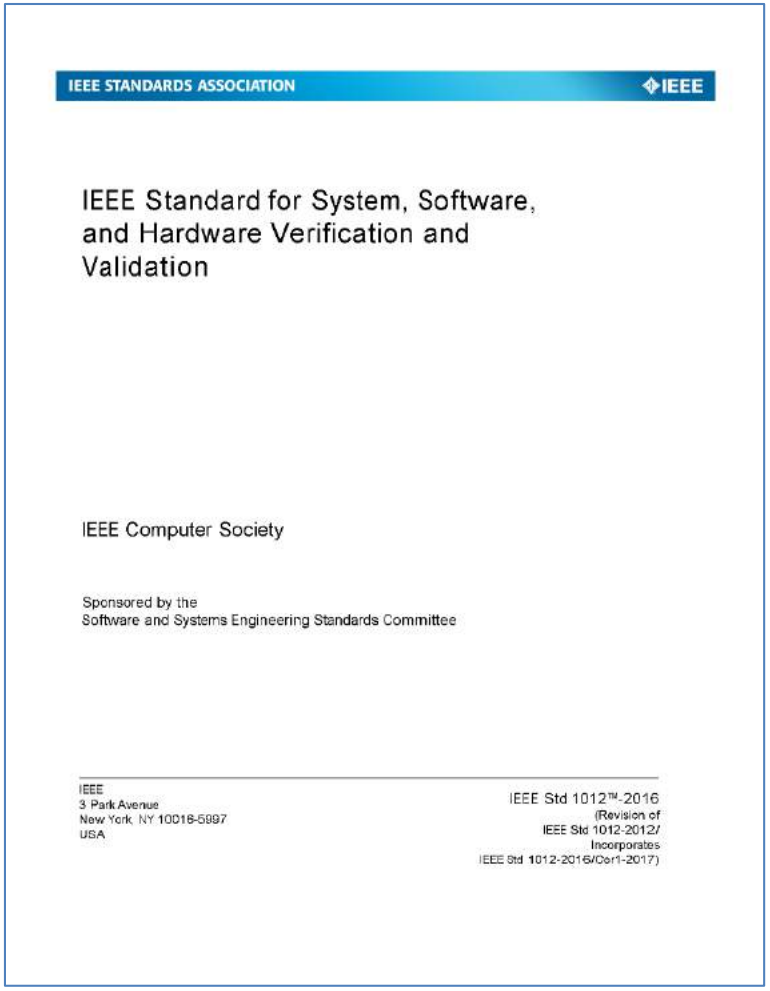
- how one should use the standard and apply adaptations for FPGA technology
- the impacts of necessary adaptations for FPGA technology and the use of the standard for regulatory purposes, since individual adaptations by vendors and plant operators dilutes the value of the standard
- thoughts on how IEEE 1012 can be or should be used for projects based on FPGA technologies developed to IEC standards since most vendor platforms

Some Problems Have Two Solutions

$$X^2 = 4$$

IMPERIA
ENGINEERING PARTNERS

IEEE 1012 Today


IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for System, Software, and Hardware Verification and Validation

IEEE Computer Society

Sponsored by the
Software and Systems Engineering Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1012™-2016
(Revision of
IEEE Std 1012-2012/
Incorporates
IEEE Std 1012-2016/Cor1-2017)

"IEEE Std 1012 is a process standard that defines the V&V processes in terms of specific activities and related tasks. The standard also defines the contents of the V&V plan."

(from Introduction)

IMPERIA ENGINEERING PARTNERS

V&V Use History

Vehicle Registration and Licensing System

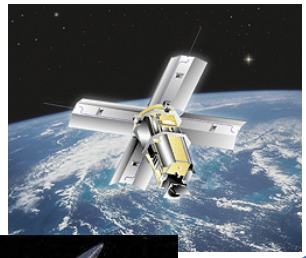
Nuclear Power Plant Instrumentation & Control

Healthcare Respiratory Monitoring System

Manned Space Missions

Air Traffic Control

Satellite Systems



Critical Space Missions

Radiation Therapy Devices

- *Self Driving Automobile System*
- *Financial/Banking*
- *Robotic Surgery*
- *Automated Voting Systems*
- *Smart Grid Networks*
- *Cyber security*
- *Cloud Security*

Missile Launch Systems

1960's 1980 1990 2000 2010 2015

IMPERIA ENGINEERING PARTNERS

V&V Processes

- Determine whether
  - development products conform to requirements
  - system-of-interest satisfies its intended use and user needs
- May include
  - analysis
  - evaluation
  - review
  - inspection
  - assessment
  - testing

IEEE 1012 Evolution

Year	Title
1986	IEEE Standard for Software Verification and Validation Plans
1998	IEEE Standard for Software Verification and Validation
2004	IEEE Standard for Software Verification and Validation
2012	IEEE Standard for System and Software Verification and Validation
2016	IEEE Standard for System, Software, and Hardware Verification and Validation

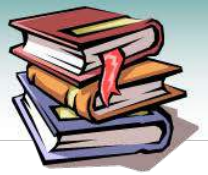
IMPERIA
ENGINEERING PARTNERS

IEEE 1012 Evolution (cont.)

1012-1986

- Plan Standard
- Critical/Non Critical
- Required Tasks
- Optional Tasks
- Format of V&V Plan
- 27 pages

1012-1998

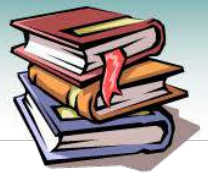


- ISO/IEC 12207
- Process Standard
- SW Integrity Levels
- Required Tasks/Levels
- Elaboration of Tasks (Table 1)
- Entry/Exit Criteria
- Notions on:
  a) V&V Metrics
  b) Reuse Software
- Definition of IV&V
- Sample Organization Chart (V&V, QA, Sys Engr)
- 71 pages

1012- 2004

- Continued Process
- Broad industry application
- State of the Art V&V Practices
  a) Reused SW
  b) Metrics
  c) Process Improvement (CMMI)
- Systems Viewpoint
- Measures of V&V effectiveness and efficiency
- 110 pages

1012-2012



- ISO/IEC 15288 and 12207 Life Cycle Stds
- Broad industry application
- Systems V&V
  a) Common
  b) Systems
  c) Software
  d) Hardware
- Practices
  a) Reuse
  b) Metrics
- 221 pages

IMPERIA ENGINEERING PARTNERS

Most Recent IEEE 1012 Changes

- V&V activities/tasks address new/modified processes from ISO/IEC/IEEE 15288:2015, “Systems and software engineering – System life cycle processes”. [Conformance to IEEE 1012 aligns with conformance to ISO/IEC/IEEE 15288’s V&V clauses.]
- Terminology/structure/mappings consistent with ISO/IEC/IEEE 15288:2015

IEEE 1012 Key Concepts

- Integrity levels
- Minimum V&V tasks for each integrity level
- Optional V&V tasks
- Intensity and rigor applied to V&V tasks
- Detailed criteria for V&V tasks
- Systems viewpoints
- Alignment with other software and systems engineering standards,

Use of IEEE 1012

- Broadly applicable & highly flexible
  - Used in many industry and government sectors
  - Used for bespoke and COTS/GOTS systems
  - Used at platform/integration/application levels
  - Adaptable to various types of programmable electronic equipment (including FPGAs)
  - Compatible with all life cycle models

What Wags What?

V&V Processes (tail)

Life Cycle Processes (dog)

Don’t let the V&V processes “tail” wag the life cycle processes “dog”!

Life Cycle Processes / V&V Processes

- “This standard is compatible with all life cycle models … ; however, not all life cycle models use all of the processes listed in this standard.”
- “The user of this standard may invoke those life cycle processes and the associated V&V processes that apply to the project.”
- (both from IEEE 1012 Subclause 1.1

So Why Does IEEE 1012 *Seem Like* a Life Cycle Process Standard?

- At the core of IEEE 1012 are the V&V tasks and their detailed criteria, which cannot be written without organization and structure.
- Industry standards provide comprehensive listings of all life cycle processes that could be invoked for a particular project.
- It makes sense to use those life cycle process standards to provide the

Conformance to IEEE 1012

- "The V&V task criteria described in Table 1a through Table 1d explicitly define the conformance requirements for V&V processes." (from Subclause 1.1 Scope)
- "If a project uses only selected lifecycle processes, then conformance to this standard is achieved if the minimum V&V tasks are implemented for all of the associated lifecycle processes selected for the project." (from Subclause 1.7 Conformance)

Conformance to IEEE 1012 (cont.)

- "Specific development methods and technologies … may eliminate development steps or combine several development steps into one; therefore, a corresponding adaptation of the minimum V&V tasks is permitted and is documented in any claim of conformance to this standard." (from Subclause 1.7 Conformance)

Conformance to IEEE 1012 (cont.)

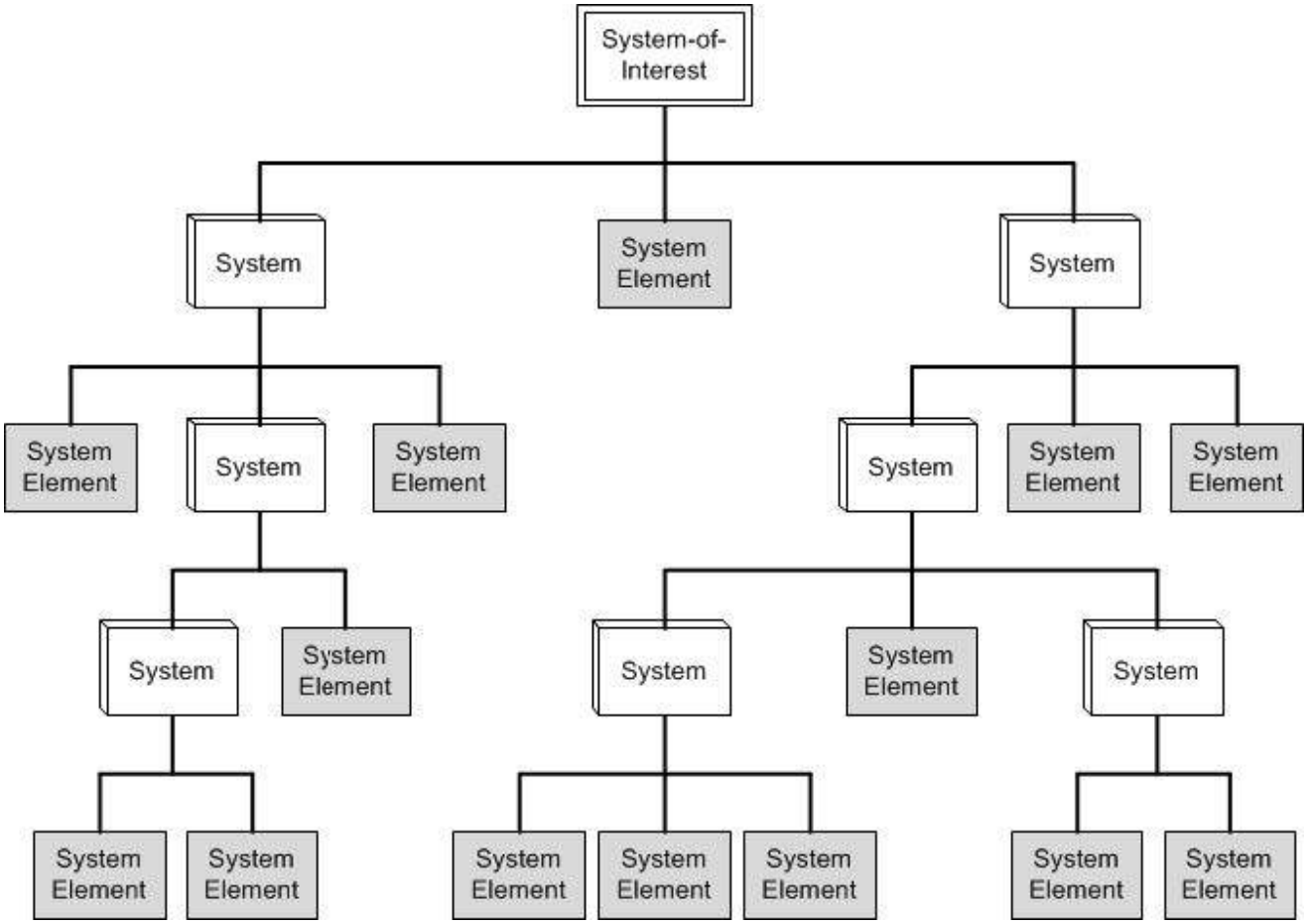
- “Not all projects include each of the life cycle processes listed. To conform to this standard, the V&V processes shall address all those life cycle processes used by the project.” (from Subclause 6.1 General)

IMPERIA ENGINEERING PARTNERS

Applying IEEE Std 1012 to FPGAs

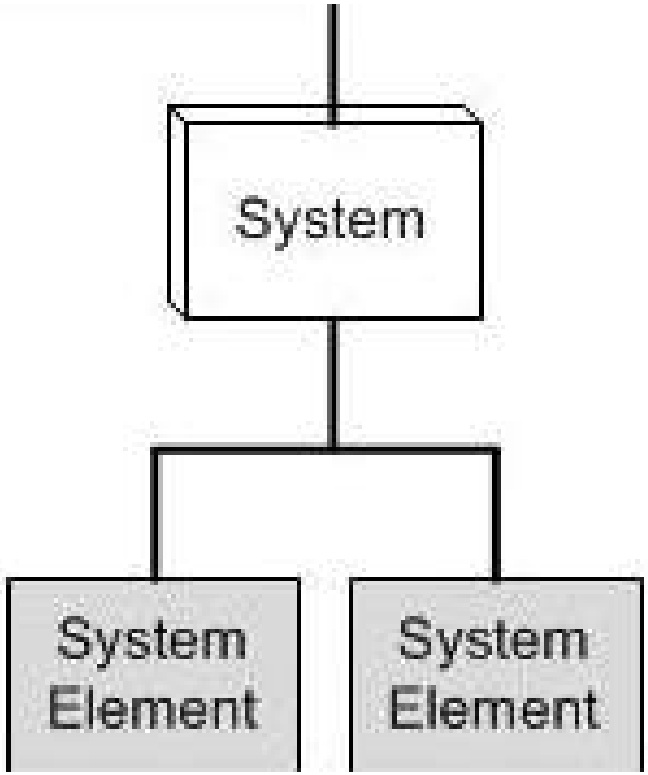
- "The V&V standard is applied recursively within the concept of a system of systems and from system to software or hardware components." (from Subclause 1.5 Organization of the standard)
- This is not an easy concept to grasp. What does it mean?

IEEE 1012 Figure 4, “Example system-of-interest structure”



IMPERIA ENGINEERING PARTNERS

FPGA Example (lower right corner of previous slide)



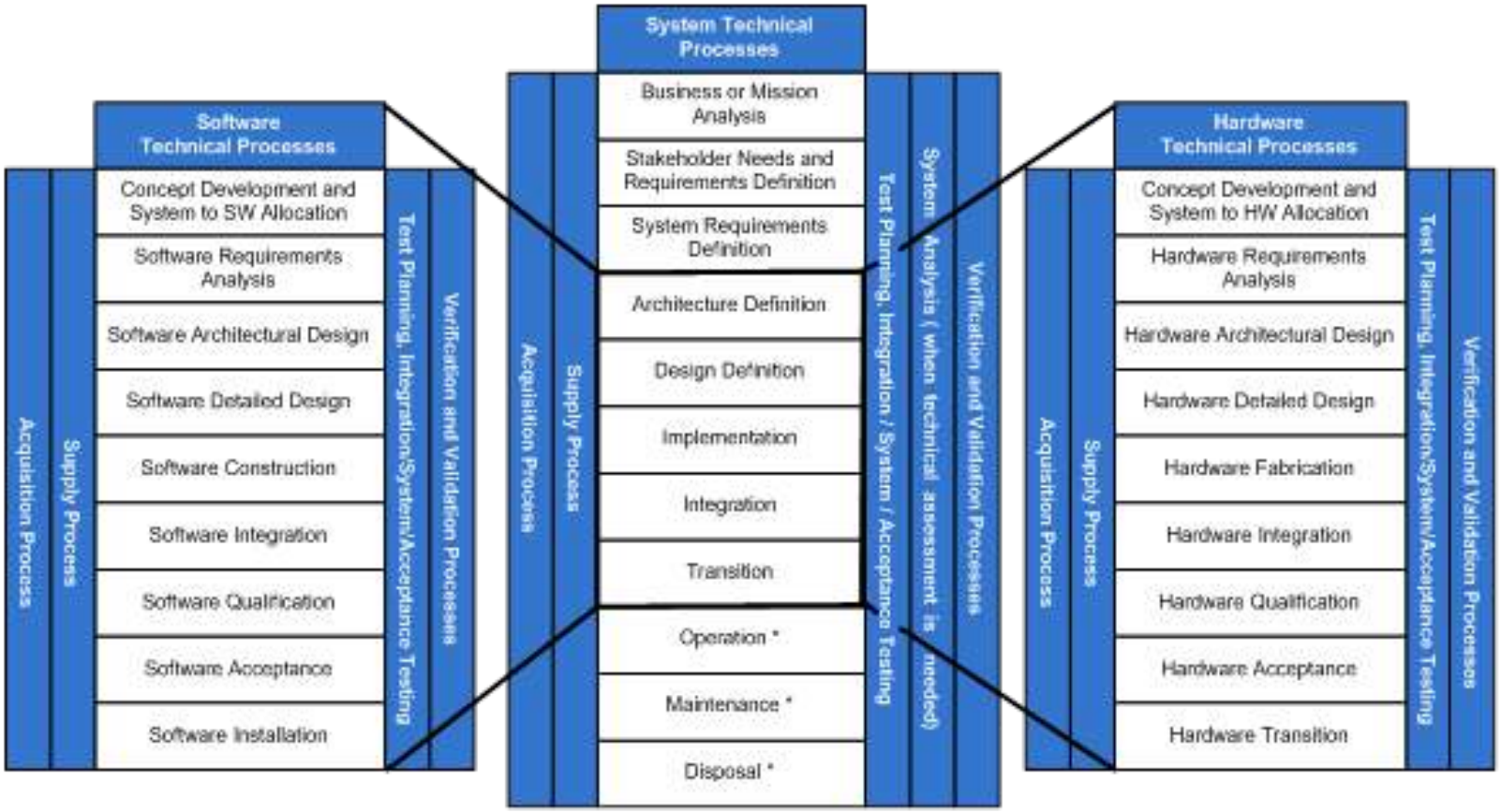
Consider the “System” to be the smallest entity that contains the fully integrated FPGA.
Use Clause 8 System V&V processes

Consider the first “System Element” to be the HDL program (prior to integration with HW).
Use Clause 9 Software V&V processes

Consider the second “System Element” to be the “System” prior to FPGA programming.
Use Clause 10 Hardware V&V processes

IMPERIA ENGINEERING PARTNERS

IEEE 1012 Figure 5, “Relationship of system, software, and hardware processes”



IMPERIA ENGINEERING PARTNERS

IEEE 1012 Figure 8, “Minimum level for V&V testing by integrity level”

IMPERIA
ENGINEERING PARTNERS

Lots of Choices to Document

- “The V&V effort shall generate a VVP that addresses the topics described in Clause 12 of this standard … The VVP shall be maintained throughout the life cycle of the system, software, or hardware.” (from Subclause 11.3.2 VVP documentation)
- “If the life cycle used in the VVP differs from the life cycle model in this standard, this section shall describe how all requirements of the standard are satisfied.” (from Subclause 12.5.2 VVP Section 4.2: Master schedule)

But We Use the 2004/1998 Version

- IEEE 1012-2004 (and -1998) is still widely used in the nuclear power industry.
- Compliance with IEEE 1012-2016 likely encompasses older versions' requirements.
- The systems engineering approach of IEEE 1012-2016 is *superior* to that of the older, software focused versions.
- Recommendation: Use IEEE 1012-2016

Other Objections & Responses

Objection	Response
IEEE 1012's development life cycle must be adapted for an IEC standards-driven FPGA development life cycle.	IEEE 1012 does not dictate any development life cycle. An IEC standards-driven life cycle does not preclude using IEEE 1012 for V&V.
IEEE 1012's recurring criticality analyses have no value for nuclear SR systems.	State in the VVP that the system-of-interest is integrity level 4 throughout the project and, therefore, criticality analyses will not be repeated.
IEEE 1012's security analyses are redundant to those performed to satisfy other regulatory requirements.	Security analysis V&V tasks performed by non-V&V team members may be credited in the VVP, with reference(s) to the applicable documentation.
IEEE 1012's V&V tasks need adaptation to include FPGA-specific requirements.	The IEEE P1012 WG is evaluating the possible addition of FPGA-specific V&V tasks and/or criteria.

In-Progress IEEE 1012 Revision

- Align SW and HW clauses to ISO/IEC/IEEE 12207:2017 (which has been aligned to ISO/IEC/IEEE 15288:2015)
- Addition of a handful of vignettes to illustrate integrity level assignments (one deals with nuclear power)
- Integration of results from numerous assigned topics (one of which is FPGAs)

Assigned Topic on FPGAs

- Items Being Considered:
  - Guidance on boundaries for applying system V&V processes vs software V&V processes vs hardware V&V processes
  - FPGA-specific V&V task criteria
  - Address tool verification
  - Simulation test planning during requirements definition V&V processes
  - Concepts from IEC 62566

Next IEEE P1012 WG Meeting

- November 6-8, 2019
- Hosted by NuScale Power
- Corvallis, Oregon (USA)
- Special group hotel rate available until October 16, 2019
- Please see me if you are interested in providing your thoughts and/or participating on the working group.

Questions