Regulatory Experience in Using Int'l Standards for reviewing FPGA Systems

YONG-IL KWON (k722kyi@kins.re.kr)

I&C and Electrical Evaluation Department of KINS

Contents

Current Status of NPPs in Korea

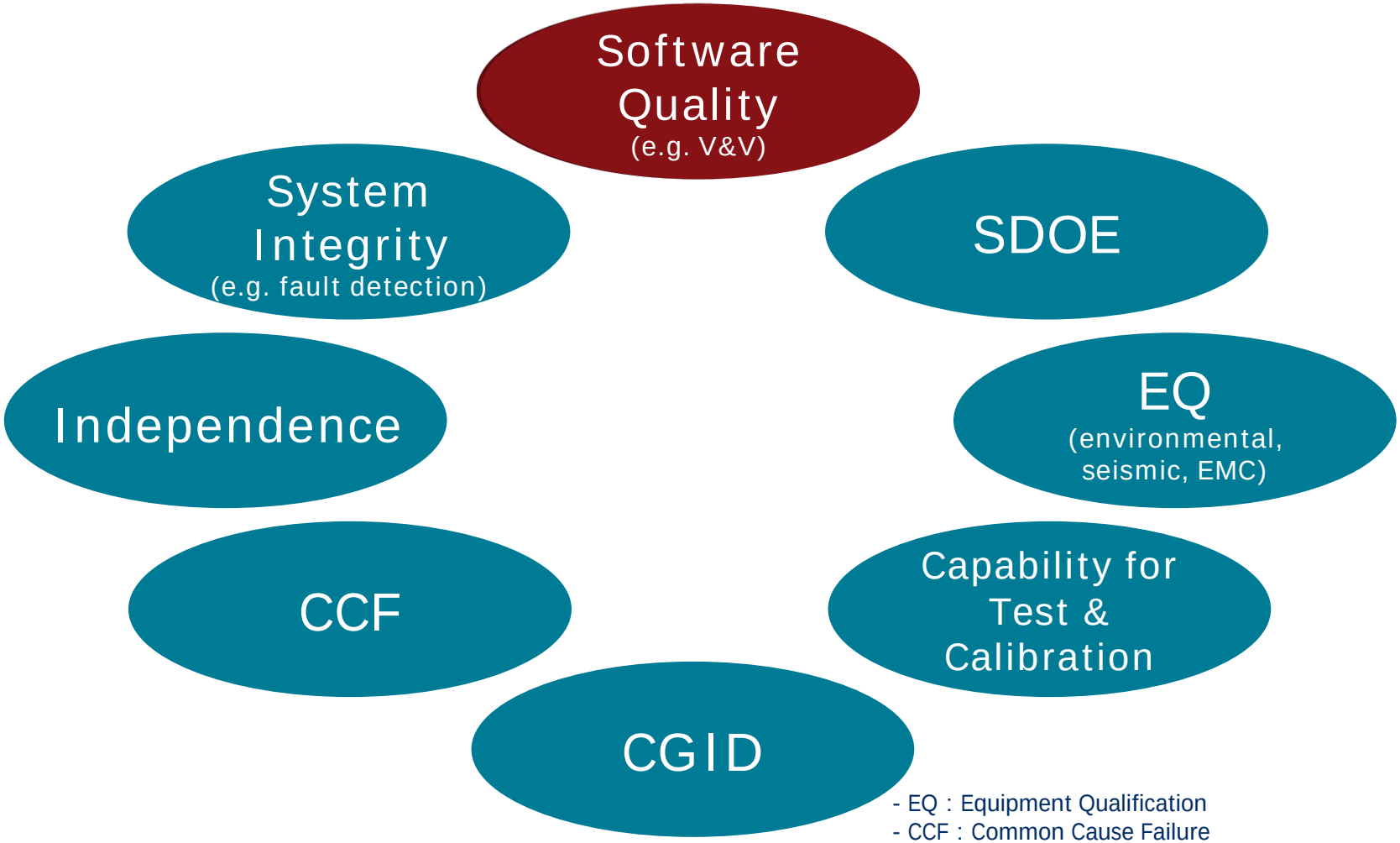
In operation

23 Units
(21,850 MW)

Under construction

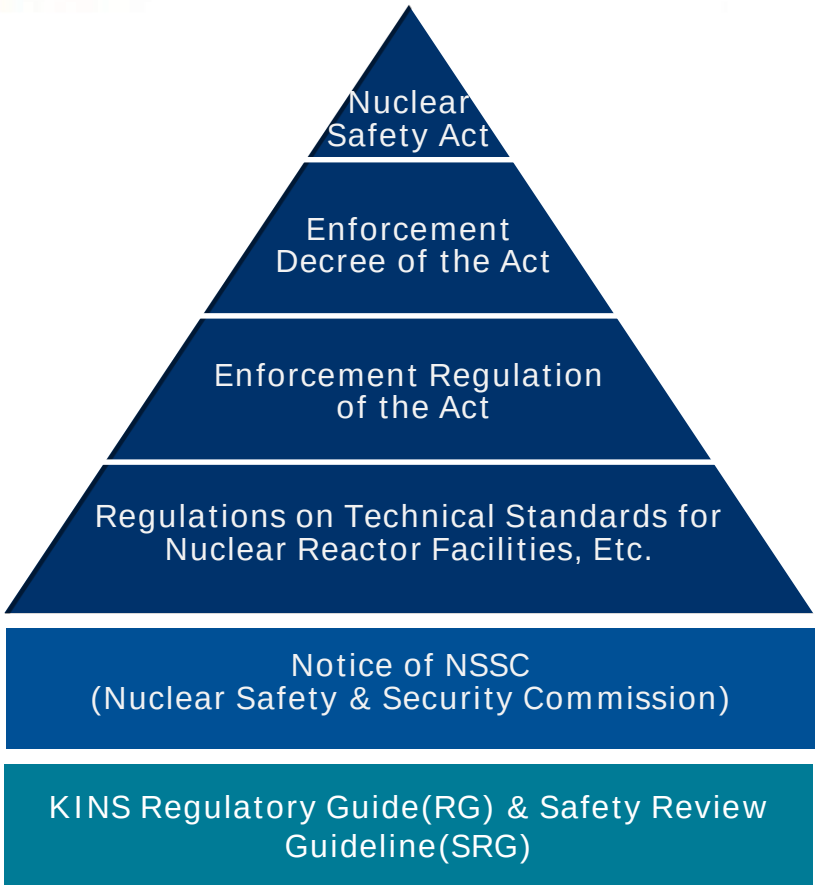
5 Units
(7,000 MW)

Topics for Reviewing Digital I&C Systems



- EQ : Equipment Qualification
- CCF : Common Cause Failure
- CGID : Commercial Grade Item Dedication
- SDOE : Secure Development & Operational Environment

Legal System of Nuclear Safety Regulation



KINS RG 8.13	• Use of Computer in Safety System • IEEE Std. 7-4.3.2
KINS RG 8.15	• SW V&V, Review/Audit • IEEE Std. 1012, 1028
KINS RG 8.16	• SW Configuration Management • IEEE Std. 828
KINS RG 8.17	• SW Test Documentation • IEEE Std. 829
KINS RG 8.18	• SW Unit Testing • IEEE Std. 1008
KINS RG 8.19	• SW Requirement Spec. • IEEE Std. 830
KINS RG 8.20	• SW Life Cycle Process • IEEE Std. 1074
KINS RG 17.12	• CGID • EPRI TR-106439
KINS SRG 7-13	• SW Review for Digital I&C System • NRC BTP 7-14
KINS SRG 7-15	• Use of PLC in Digital I&C System • EPRI TR-107330

Int'l Standards and Reports for FPGA Systems

- IEC 62566, "Nuclear Power Plants - Instrumentation and Control Important to Safety - Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions", 2012
- IAEA, No. NP-T-3.17, "Application of Field programmable Gate Arrays in Instrumentation and Control Systems of NPPs", 2016
- NUREG/CR-7006, "Review Guidelines for FPGAs in NPP Safety Systems", 2010
- EPRI TR-1019181, "Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems", 2009
- OECD/NEA MDEP(Multinational Design Evaluation Program), Generic Common Position, No. DICWG-04, "Common Position on the Treatment of HDL-programmed Devices for Use in Nuclear Safety Systems", 2013

Documents in S/W Life Cycle

◆ NRC SRP BTP 7-14, "Guidance on S/W Reviews for Digital Computer-Based I&C Systems"

Planning	Require.	Design	Implement.	Integration	Validation	Installation	Operation/ Maintenance
• Management • Development • QA • Integration • Installation • Maintenance • Training • Operation • Safety • V&V • Test • CM	• Requirement Specification	• Design Specification • H/W, S/W Architecture	• Coding Listings	• System Build Documents		• Operation, Maintenance and Training Manuals • Installation Configuration Tables	
	Design Outputs						
	For each life cycle phase • Safety Analysis • V&V(Verification & Validation) • CM(Configuration Management)						
Process Planning	Process Implementation						

V&V Activities

◆ IEEE Std. 1012, "IEEE Standards for S/W Verification and Validation"

Requirement	Design	Implementation/ Integration	Validation(Test)
• Traceability Analysis	• Traceability Analysis	• Traceability Analysis	• Traceability Analysis
• Security Analysis	• Security Analysis	• Security Analysis	• Security Analysis
• Hazard/Risk Analysis	• Hazard/Risk Analysis	• Hazard/Risk Analysis	• Hazard/Risk Analysis
• Requirement Evaluation	• Design Evaluation	• Source Code Evaluation	
• Test Plan	• Test Plan	• Test Procedure	• Test Procedure
- System	- Component	- Component	- Acceptance
- Acceptance	- Integration	- Integration	• Test Execution
		- System	- Integration
		• Test Execution	- System
		- Component	- Acceptance

Use of IEC 62566 (1/2)

Phase	SRP BTP 7-14 & IEEE Std. 1012	Related **Int'l Standards**	IEC 62566
Requirement	• Requirement Specification & Evaluation	• IEEE Std. 7-4.3.2 • IEEE Std. 830	Clause 6, "HPD Requirements Specification"
Design	• Design Outputs(e.g. design spec., code) & Evaluation	• IEEE Std. 7-4.3.2 • IEEE Std. 829 • IEEE Std. 1008	Clause 8, "HPD Design & Implementation"
Implement., Integration	• Component Test Documents(e.g. plan, procedure)		Clause 9, "HPD Verification"
Validation (Test)	• Integration Outputs & Evaluation • Integration Test Documents	• IEEE Std. 7-4.3.2 • IEEE Std. 829	Clause 10, "HPD aspects of System Integration"
	• System Test Documents		Clause 11, "HPD aspects of System Validation"
	• Acceptance Test Documents		Clause 13, "HPD Production"

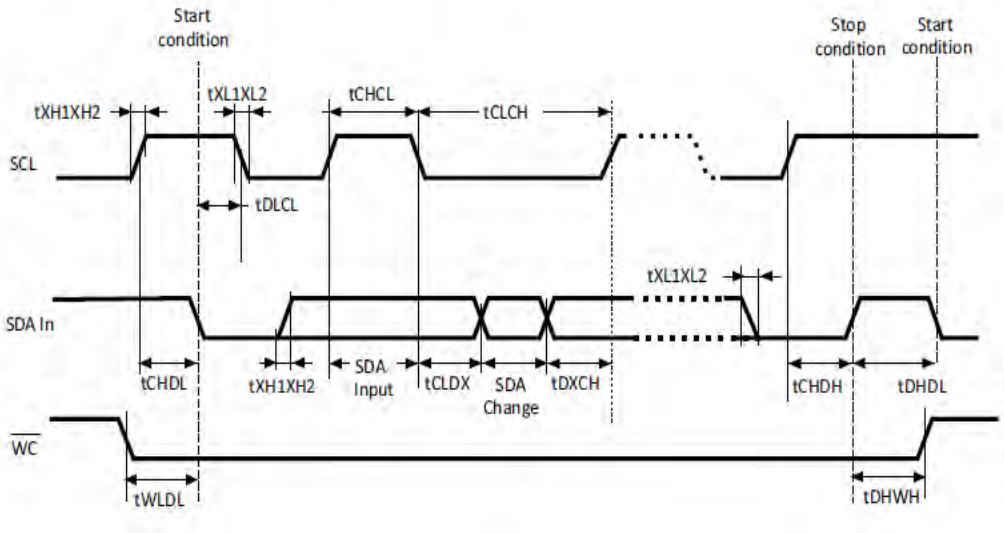
Use of IEC 62566 (2/2)

◆ The existing standards for the below topics can be fully applied to both 'FPGA' and 'micro-processor'. No more requirements for the topics are necessary.

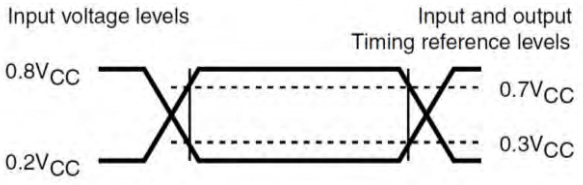
Other Topics of IEC 62566	Existing Standards for Digital I&C Systems
S/W Life Cycle Process (Clause 5)	• IEEE Std. 1074
S/W QA Plan (Clause 5)	• IEEE Std. 730
S/W CM Plan (Clause 5)	• IEEE Std. 828
CGID (Clause 7)	• EPRI TR-106439, 3002002982 • NRC RG 1.164
S/W Tool Qualification (Clause 15)	• IEEE Std. 7-4.3.2
CCF (Clause 17)	• IEEE Std. 7-4.3.2 • NRC SRP BTP 7-19

Key Requirements in Requirement Phase

- The followings shall be documented in the requirement specification.
  - ▷ electrical and temporal performance(e.g. setup/hold time, operating frequency)
  - ▷ profiles of interfaced signal and power supplies
  - ▷ operating temperature
- Example : EEPROM(I^2C Bus) Datasheet



< Interface Profiles >



< Electrical Characteristics>

Symbol	Parameter	Min.	Max.	Unit
V_{CC}	Supply voltage	1.8	5.5	V
T_A	Ambient operating temperature	–40	85	°C

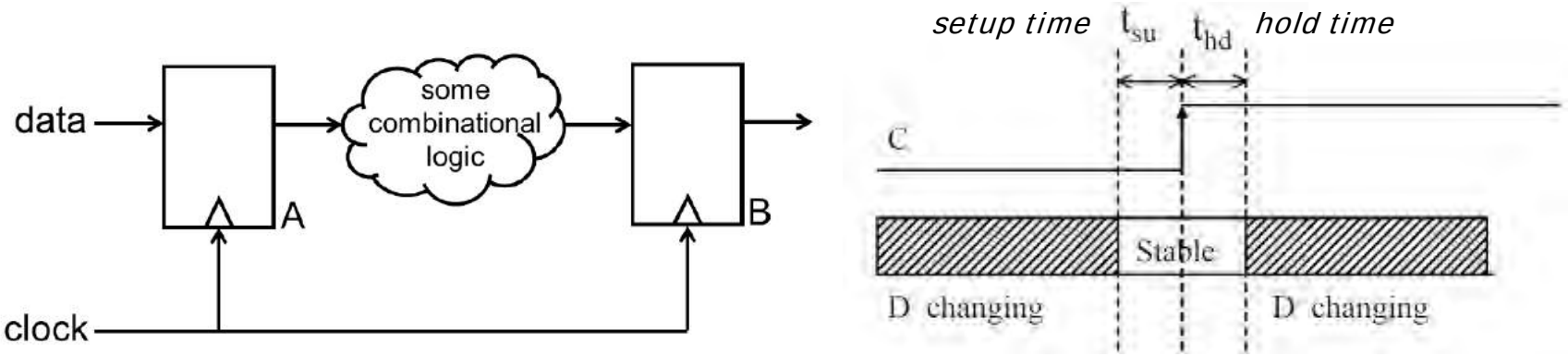
< Operating Conditions >

Key Requirements in Design/Implementation

- A synchronous architecture should be used. If not, all paths shall be analyzed.
- Post-syn. and post-P&R netlists shall be functionally equivalent to the RTL description.
  - ▷ S/W tools may remove intended logic circuits for optimization.
- Constraints and parameters used in software tools(e.g. synthesis, P&R) shall be verified and placed under configuration management.
- All the features(e.g. functions, operation modes) mentioned in requirement specification and design specification shall be simulated in the component test.
- The test bench should have 100% code coverages for statement, branch, expression (condition) and FSM. If not, the documented justification shall be produced.
- The timing simulation and STA(Static Timing Analysis) for post-P&R netlist shall be performed for both "worst case" (setup time violation) and "best case" (hold time violation).

Key Requirements in Validation(1/2)

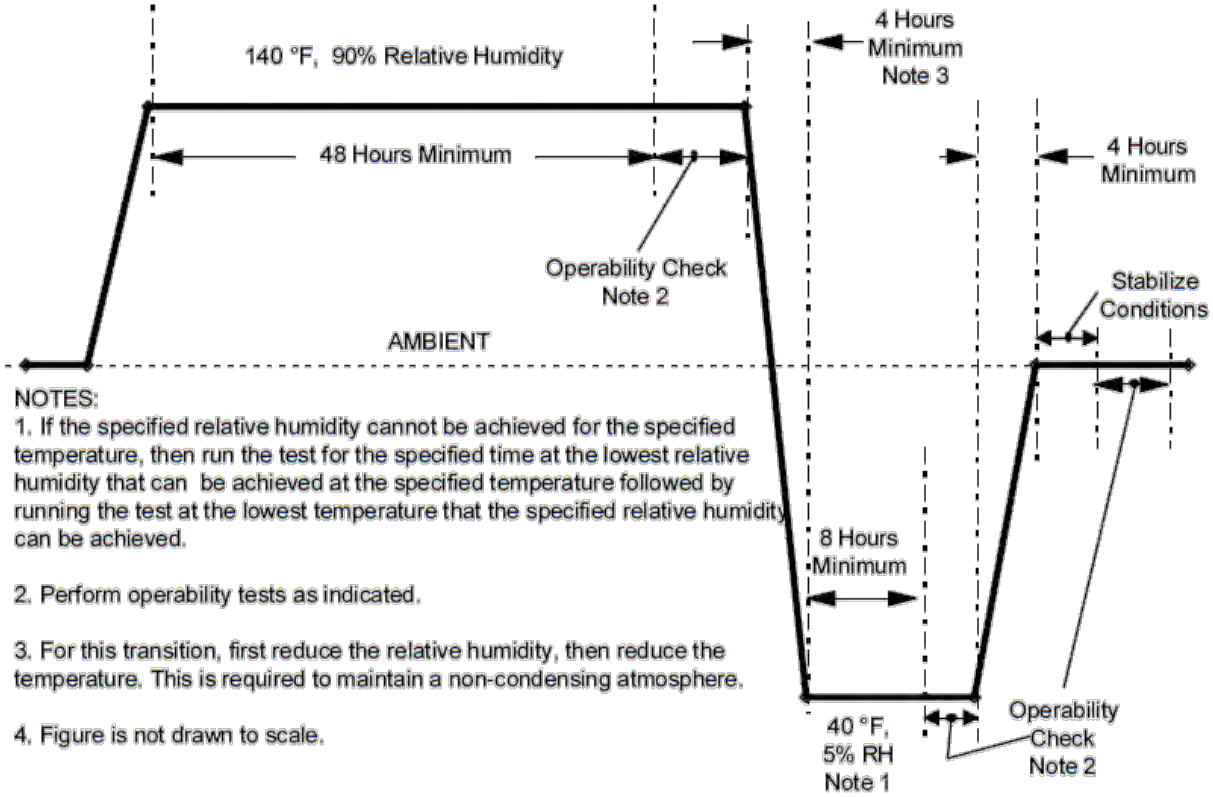
- Testing shall be performed to validate the real FPGA performance(functional, temporal, and electrical) described in requirement specification and design specification through measuring FPGA input/output signals.
- The equipment for the interface measurement shall be calibrated.
- Timing characteristics(e.g. data propagation delay, clock skew) of logic circuits are impacted by operating temperature and supply voltage.



< Setup/Hold Time >

Key Requirements in Validation(2/2)

- To ensure timing requirements are met, the type test shall be performed for normal and abnormal service conditions(e.g. temperature, supply voltage) in accordance with IEEE Std. 323 and EPRI TR-107330.



< Temp./Humidity Profile of EPRI TR-107330>

Under Review : DFLC(Doosan FPGA Logic Controller)

- Software Classification : SIL 4 of IEEE Std. 1012(Safety-Critical, Class 1E)
- Target System : I&C safety system of PWR plants
- Application for approval of 2 topical reports
  - ▷ 2 stages : "planning ~ requirement" and "design ~ validation"
- Current Review Status for the 1st TR
  - ▷ 2nd round RAI(Request for Additional Information)
  - ▷ Reviewing the adequacy of the following documents
    - topical report
    - 12 S/W planning documents, requirement specification
    - safety analysis, V&V and CM reports in requirement phase, etc.
  - ▷ Reviewing the compliance with IEEE Std. 7-4.3.2, IEC 62566, and EPRI TR-107330
    - software tool's qualification
    - environmental/seismic qualification and EMC
    - commercial grade item dedication
    - secure development and operational environment, etc.

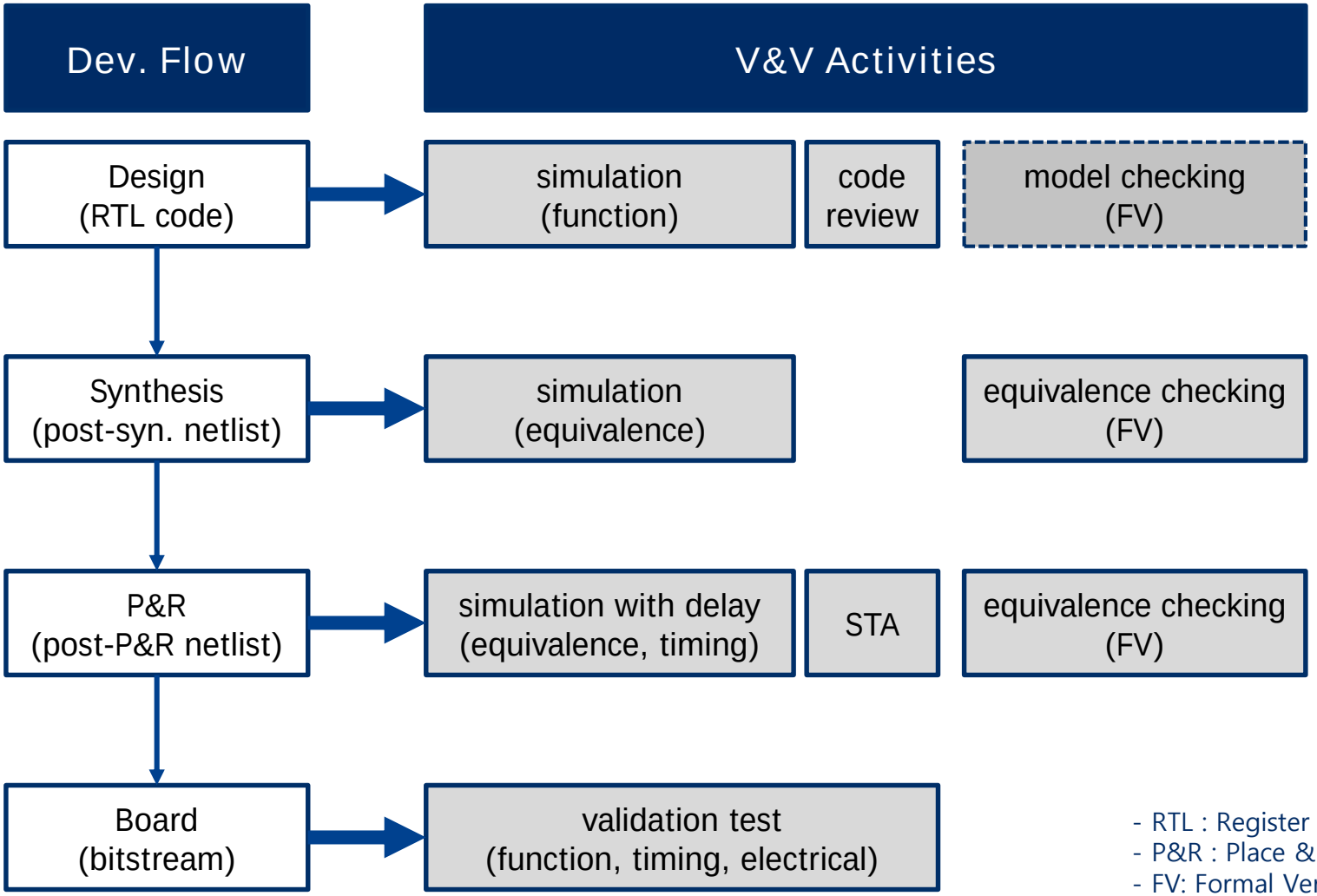
Summary

- Activities to confirm S/W quality are totally different between micro-processor and FPGA systems because FPGA is originally hardware.
- Introduce the Korean legal system for nuclear safety regulation and international standards/reports employed for reviewing S/W quality of FPGA systems.
- Explain how KINS is using IEC 62566 with the existing requirements described in NRC BTP 7-14 and IEEE Std. 1012.
- Present the key requirements for FPGA systems in each phase of life cycle.
- Talk about KINS current status for reviewing the FPGA system(DFLC).

Q&A, Comment

KINS
KOREA INSTITUTE OF NUCLEAR SAFETY

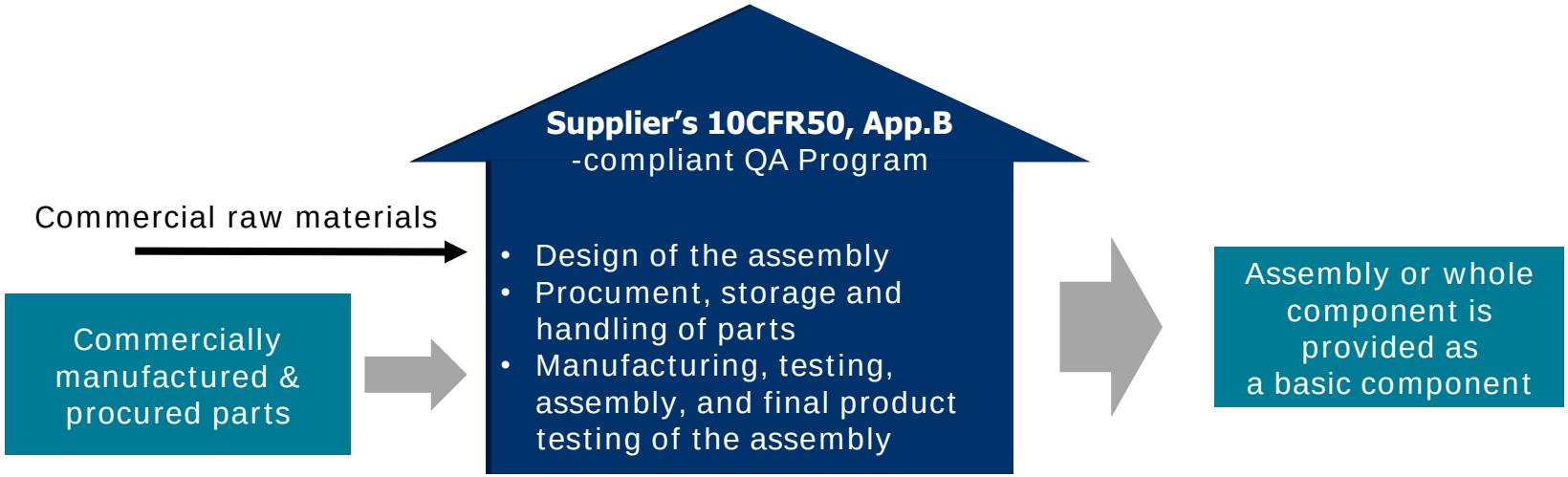
FPGA Development and V&V



- RTL : Register Transfer Level
- P&R : Place & Route
- FV: Formal Verification
- STA: Static Timing Analysis

Use of Pre-developed Items(1/2)

- If PDIs are used in the FPGA-based systems, the followings shall be met.
- In case of H/W IP cores,
  - ▷ According to EPRI 3002002982 "Revision 1 to EPRI NP-5652 and TR-102260" which is endorsed by NRC Regulatory Guide 1.164, a supplier(who is also a manufacturer) can use procured commercial parts without CGID. And a FPGA chip is regarded as at the level of parts.



- CGID : Commercial-Grade Item Dedication
- IP : Intellectual Property

Use of Pre-developed Items(2/2)

▷ If the FPGA chip is adequately controlled under QA Program(10CFR50 App. B), the FPGA chip and its H/W IP cores can be used without CGID.

Measures shall be established to assure that purchased material, equipment, and services conform to the procurement documents. These measures shall include provisions, as appropriate, for
1) source evaluation and selection
2) objective evidence of quality
3) inspection at the contractor or subcontractor source
4) examination of products upon delivery.

▷ In case of S/W IP Cores,

- According to KINS Regulatory Guide 17.12, CGID for S/W IP Cores shall be carried out in accordance with EPRI TR-106439.

◆ If PDIs may include functions not required to implement the FPGA, such functions shall not be used within the FPGA.

Use and Qualification of S/W Tools

- One or both of the following methods shall be used to confirm that outputs of S/W tools(development, V&V) are suitable for use in safety systems.
  - ▷ defects not detected by S/W tools shall be detected by V&V activities
  - ▷ S/W tools shall be developed or procured under QA program
- The qualification process for S/W tools should take into account experience from prior use.
- S/W tools shall not change the intended functions by adding or deleting certain structures which the developers don't know.
- The intended functionality and limitations of application for all S/W tools shall be identified and documented. The S/W tools and their outputs shall not be used outside their documented functionality or limitations of application without prior justification.