Review Plan for FPGA-based Logic Controller used in Safety Systems

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

I&C and Electrical Evaluation Department of KINS

KINS is a Cornerstone for a Safe Korea

********,103/2017-12-05 23:19

Contents

Ⅰ Current Status of NPPs in Korea

Ⅱ Regulatory Basis(legal system, standards)

Ⅲ Regulatory Experience

Ⅳ Regulatory Positions

Ⅴ Summary

********,103/2017-12-05 23:19

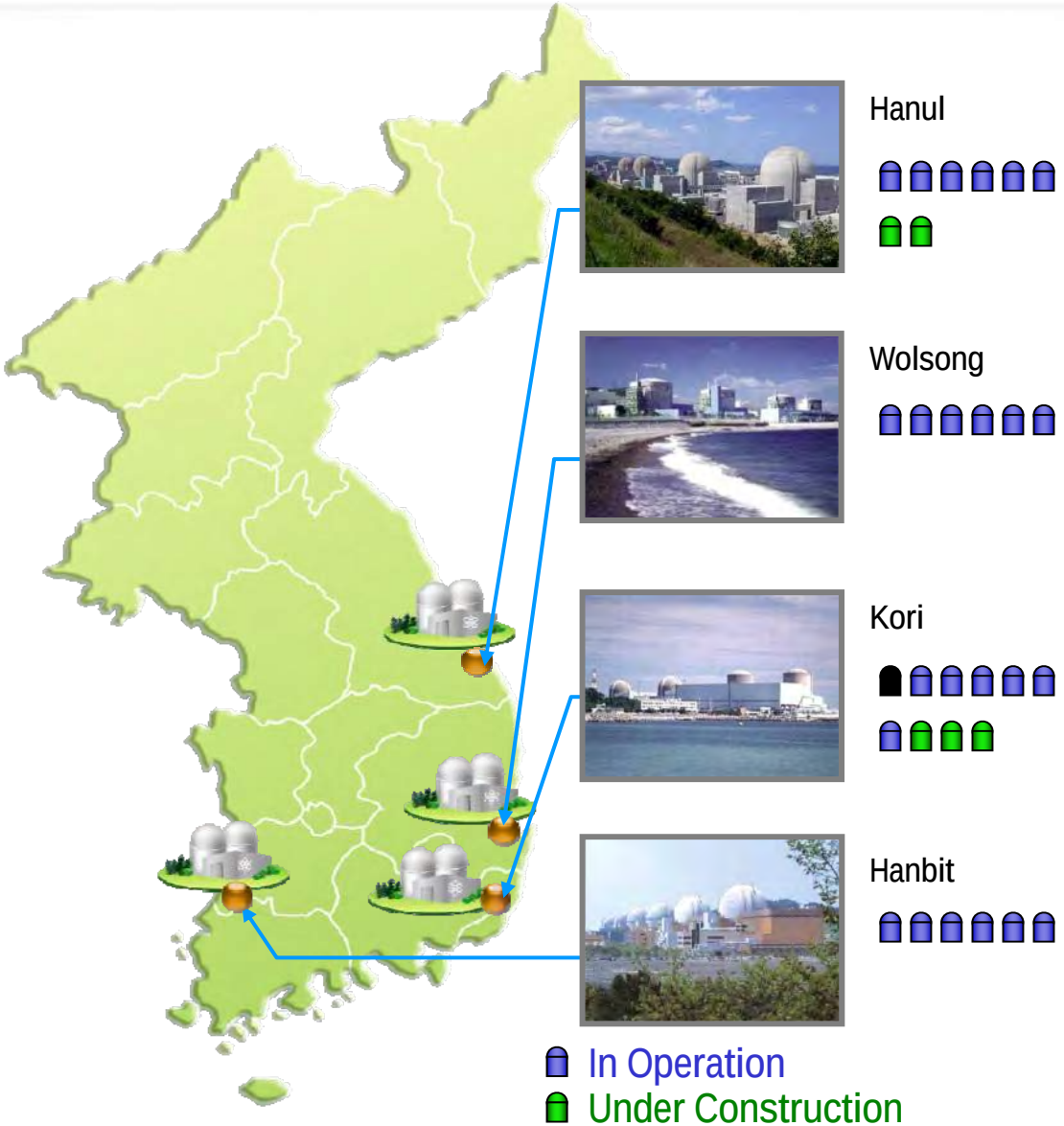
Current Status of NPPs in Korea

In operation

24 Units
(22,529 MW)

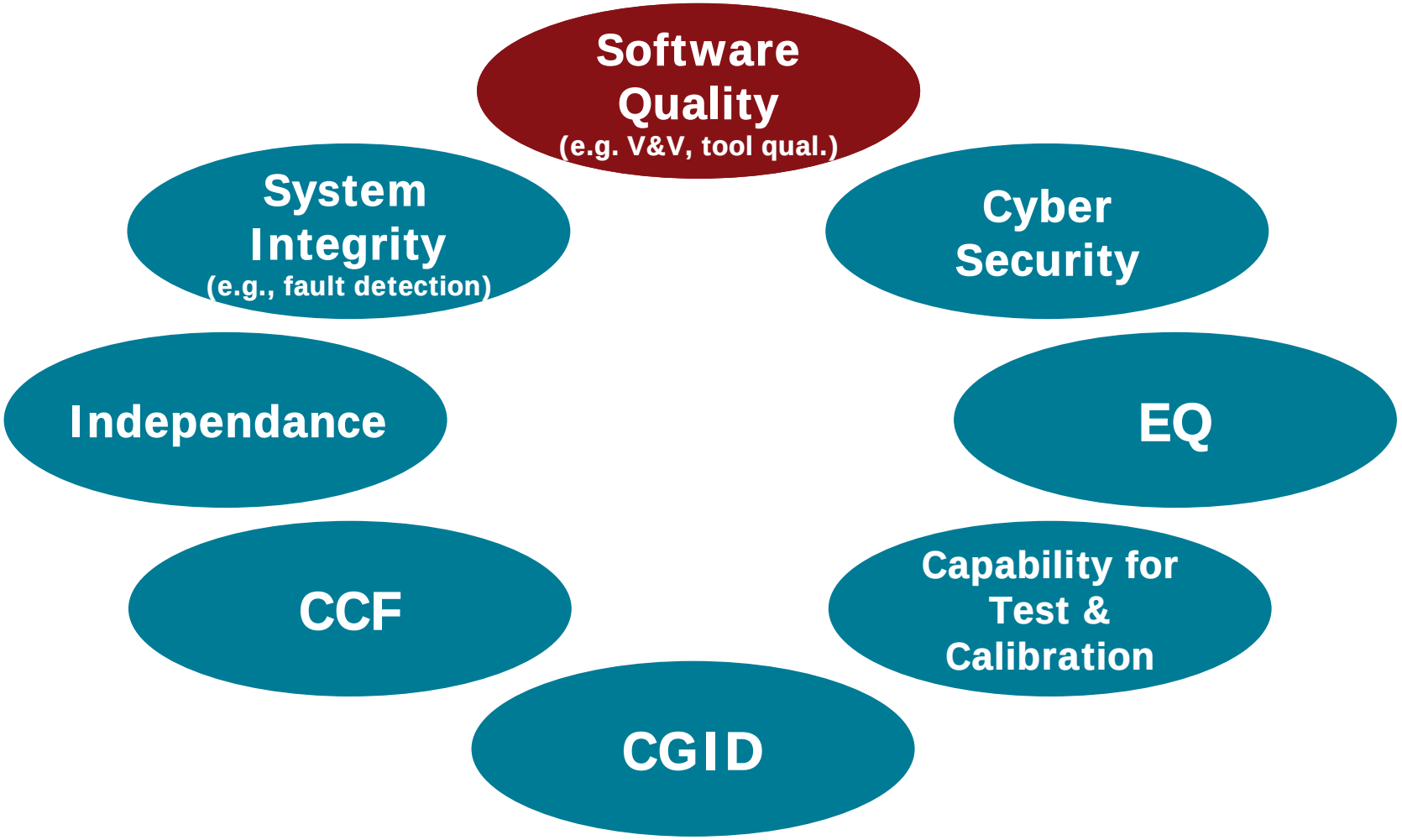
Under construction

5 Units
(7,000 MW)



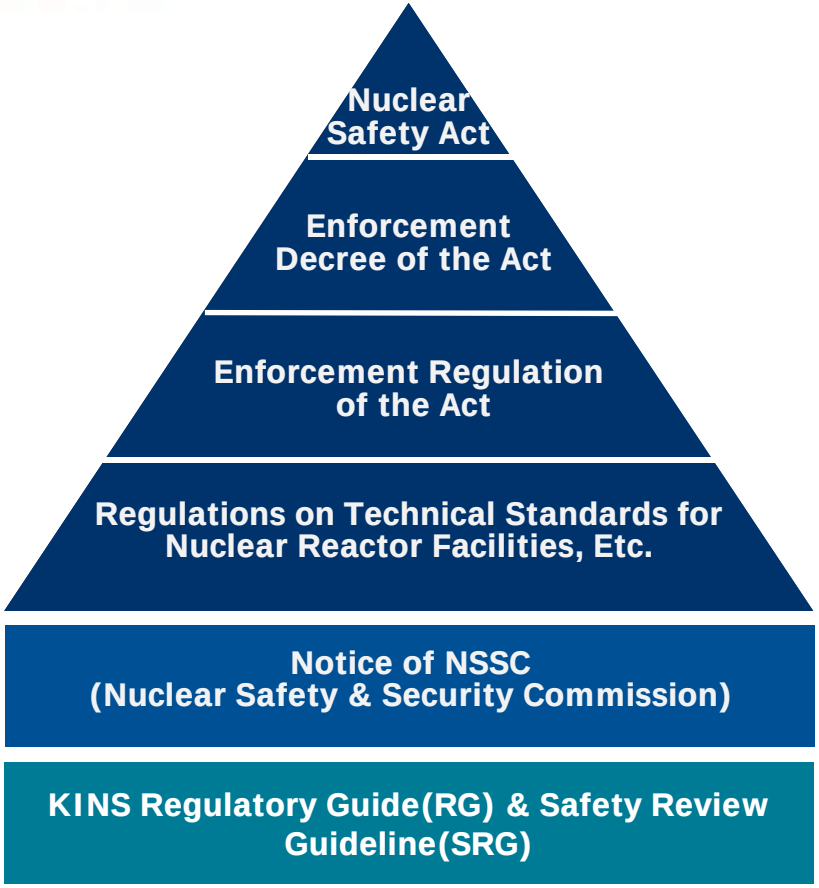
********,103/2017-12-05 23:19

Topics for Review of Digital I&C Systems



********.103/2017-12-05 23:19

Legal System of Nuclear Safety Regulation



KINS RG 8.13	● Use of Computer in Safety System ● IEEE 7-4.3.2
KINS RG 8.15	● SW V&V, Review/Audit ● IEEE 1012, IEEE 1028
KINS RG 8.16	● SW Configuration Management ● IEEE 828
KINS RG 8.17	● SW Test Documentation ● IEEE 829
KINS RG 8.18	● SW Unit Testing ● IEEE 1008
KINS RG 8.19	● SW Requirement Spec. ● IEEE 830
KINS RG 8.20	● SW Life Cycle Process ● IEEE 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

********,103/2017-12-05 23:19

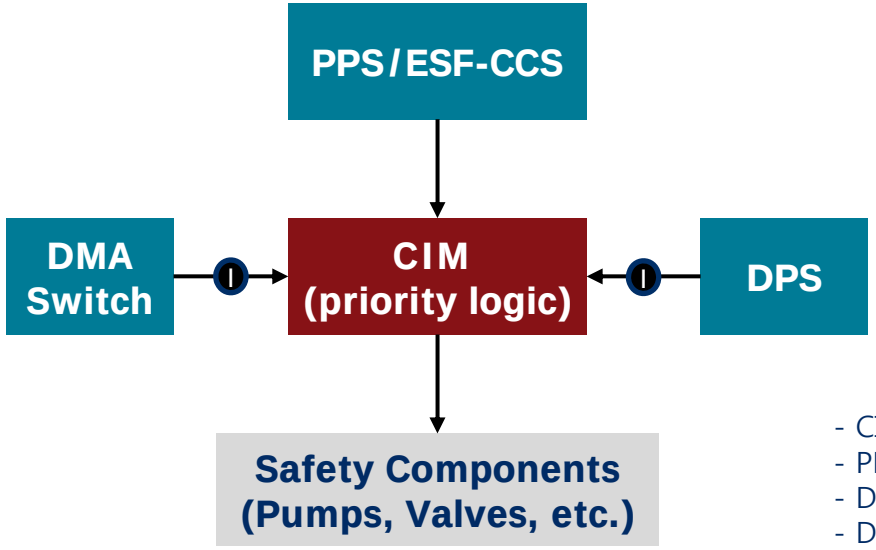
International Standards and Reports

- 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

********.103/2017-12-05 23:19

Regulatory Experience : CIM (Shin-kori Unit 3,4)

- Software Classification : SIL 4 of IEEE Std. 1012(Safety-Critical, Class 1E)
- Function : "priority logic" of component control signals from PPS, DPS and DMA



- CIM : Component Interface Module
- PPS : Plant Protection System
- DPS : Diverse Protection System
- DMA : Diverse Manual Actuation
- ESF-CCS : Engineered Safety Feature-Compoment Control System

- V&V
  - ▷ tested in the gate level of the FPGA for all possible combinations of inputs
  - ▷ independent V&V(by staff not performing the design & implementation)

********,103/2017-12-05 23:19

Regulatory Experience : FPGA-based DPS

- Software Classification : SIL 3 of IEEE Std. 1012(Non-Class 1E)
- Plant : Hanul unit 3,4,5,6, Hanbit unit 3,4,5,6
- Function : generates protective signals such as "reactor trip signal" and "AFAS (Aux. Feedwater Acuation Signal)" to cope with ATWS and S/W CCF of safety systems
- V&V
  - ▷ the simulation results for RTL code, post-synthesis netlist, and post-P&R netlist were functionally equivalent.
  - ▷ the test benches of the simulations have 100% code coverage for statement, branch, expression (condition) and FSM(Finite State Machine)
  - ▷ the simulation of post-P&R netlist was performed for worst case & best case
  - ▷ in the board-level test, the electrical I/O signals measured by logic analyser were equivalent to the simulation results in terms of the functionality
  - ▷ no IP(Intellectual Property) cores were used.

********,103/2017-12-05 23:19

Regulatory Experience : DFLC (On-going)

- ◆ Software Classification : SIL 4 of IEEE Std. 1012(Safety-Critical, Class 1E)
- ◆ Target System : I&C safety systems in PWR plants
- ◆ Application for approval of 2 topical reports of DFLC(Doosan FPGA Logic Controller)
  - ▷2 Stages : "Planning ~ Requierment" and "Design ~ Sytem Validation"
- ◆ Current Review Status
  - ▷finished the docket review of the first TR last month
  - ▷will soon launch the main review for the following documents
    - TR document
    - S/W planning document(e.g. development plan, V&V plan, QA plan)
    - requirements specification
    - requirements safety analysis report
    - V&V requirements analysis report
    - configuration management requirements report, etc.

********,103/2017-12-05 23:19

Topical Report in Korea

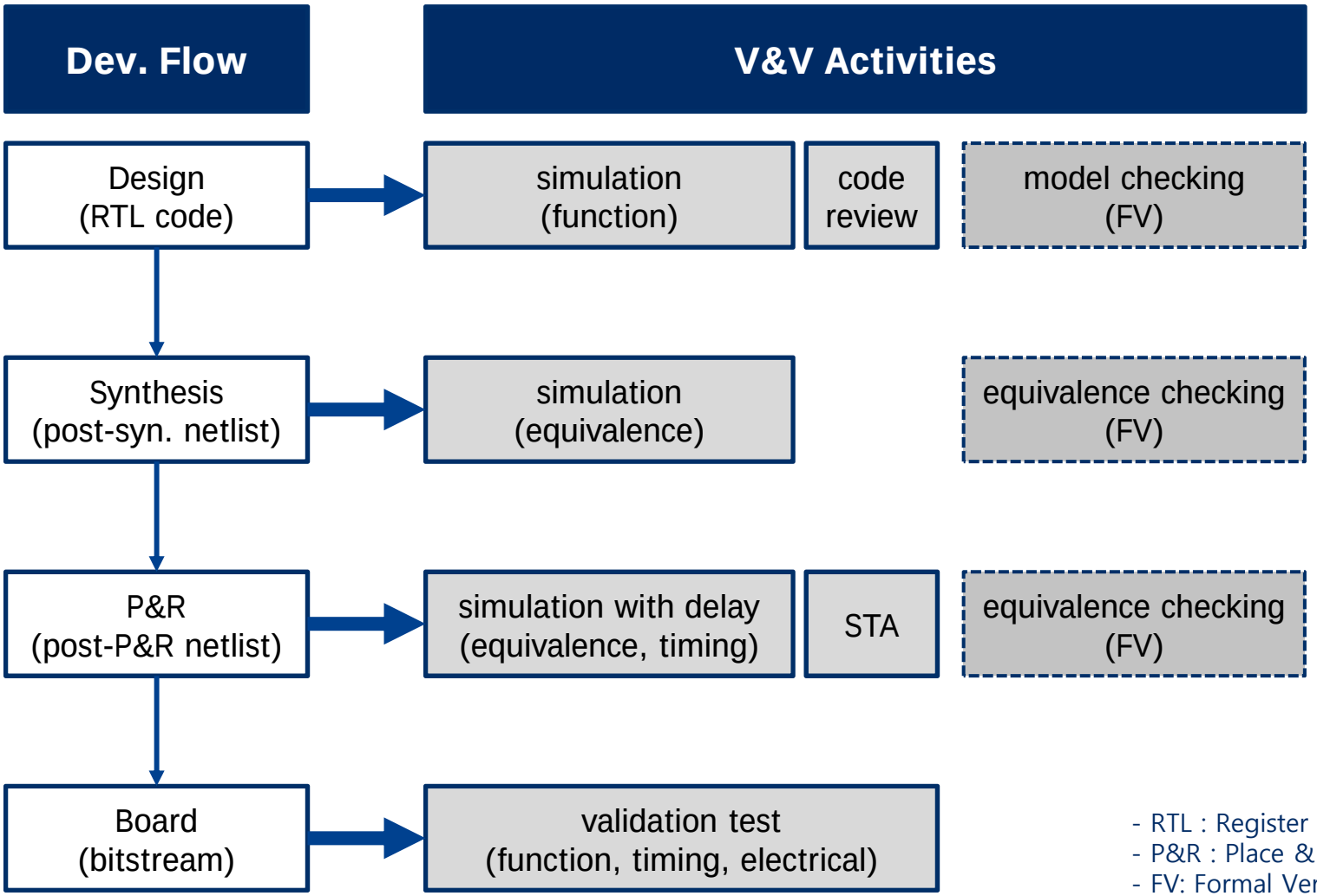
◆ Article 131(Application, etc. for Approval of Topical Report) of "Enforcement Regulation of the Act"

(1) "TR provided under the Prime Minister's Decree" under Article 100 paragraph 1 of the Decree shall refer to reports containing the information listed below:

1. Methodologies and computing codes related to technical information concerning the selection of a site for a nuclear reactor facility, design, manufacture, construction, pre-service test, trial operation, operation and disassembly
2. Information concerning safety that can be applied repeatedly for an identical purpose
3. Information that provides the basis for preparing documents to be attached to the application for a permit related to a nuclear reactor facility

********,103/2017-12-05 23:19

FPGA Development and V&V



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

********,103/2017-12-05 23:19

V&V Activities

- The simulations shall be perfomed with test benches which have 100% code coverages for statement, branch, expression(condition) and FSM.
- If the simulations don't meet the above criterion, a documented justification (e.g., reasonable reasons, complementary methods) shall be produced.
- The simulation for post-P&R netlist shall be performed for both "worst case" (setup time violation) and "best case" (hold time violation).
- If paths are excluded as "false paths" or declared as multicycle paths in STA, those paths shall be justified and documented.
- Constraints and parameters used in software tools(e.g., synthesis and P&R tool) shall be verified and placed under configuration management.

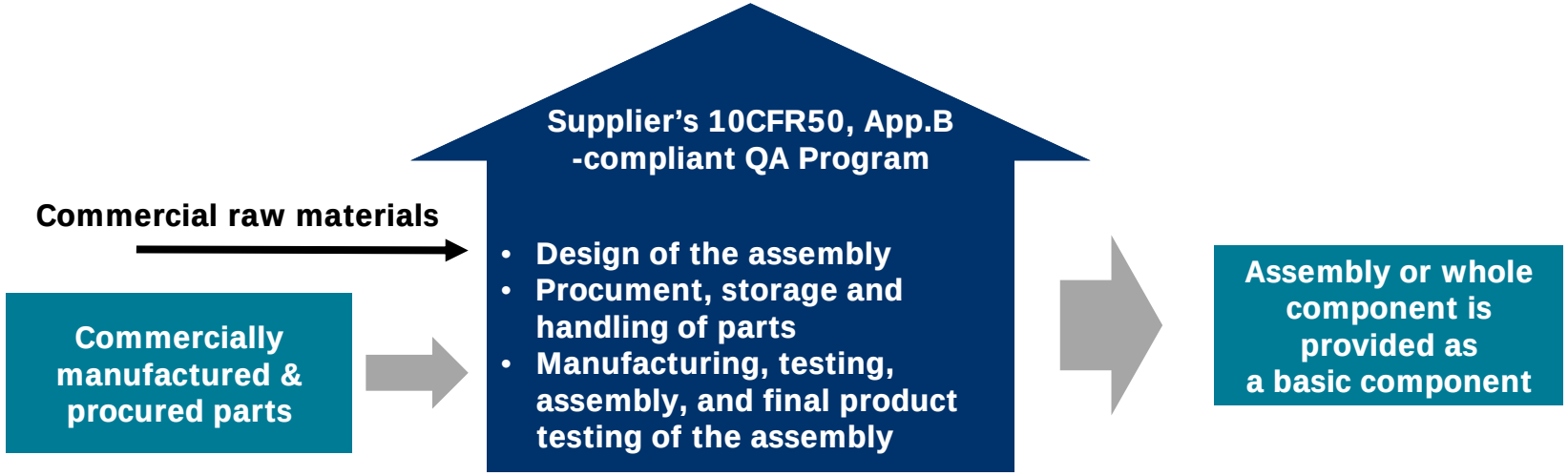
********.103/2017-12-05 23:19

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

********,103/2017-12-05 23:19

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.

********,103/2017-12-05 23:19

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.

********,103/2017-12-05 23:19

Summary

- activities to confirm S/W quality are totally different between processor-based systems and FPGA-based systems because FPGA is originally a hardware.
- introduce the Korean legal system for nuclear safety regulation and international standards and reports employed for reviewing S/W quality of FPGA-based systems.
- KINS has some regulatory experiences in evauating FPGA-based systems such as CIM, DPS and DFLC.
- explain FPGA development flow and V&V activities.
- present regulatory positions on V&V activities, use of pre-developed items and S/W tools qualification.

********.103/2017-12-05 23:19

Q&A, Comment

KINS
KOREA INSTITUTE OF NUCLEAR SAFETY

********,103/2017-12-05 23:19