Regulatory Experience in Reviewing the FPGA-based Controller in Korea

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

I&C and Electrical Evaluation Department of KINS

Contents

I Current Status of NPPs in Korea

II Regulatory Bases

III Use of International Standards

IV KINS Reg. Guide for FPGA review

V KINS Review Experience

VI Summary

Current Status of NPPs in Korea

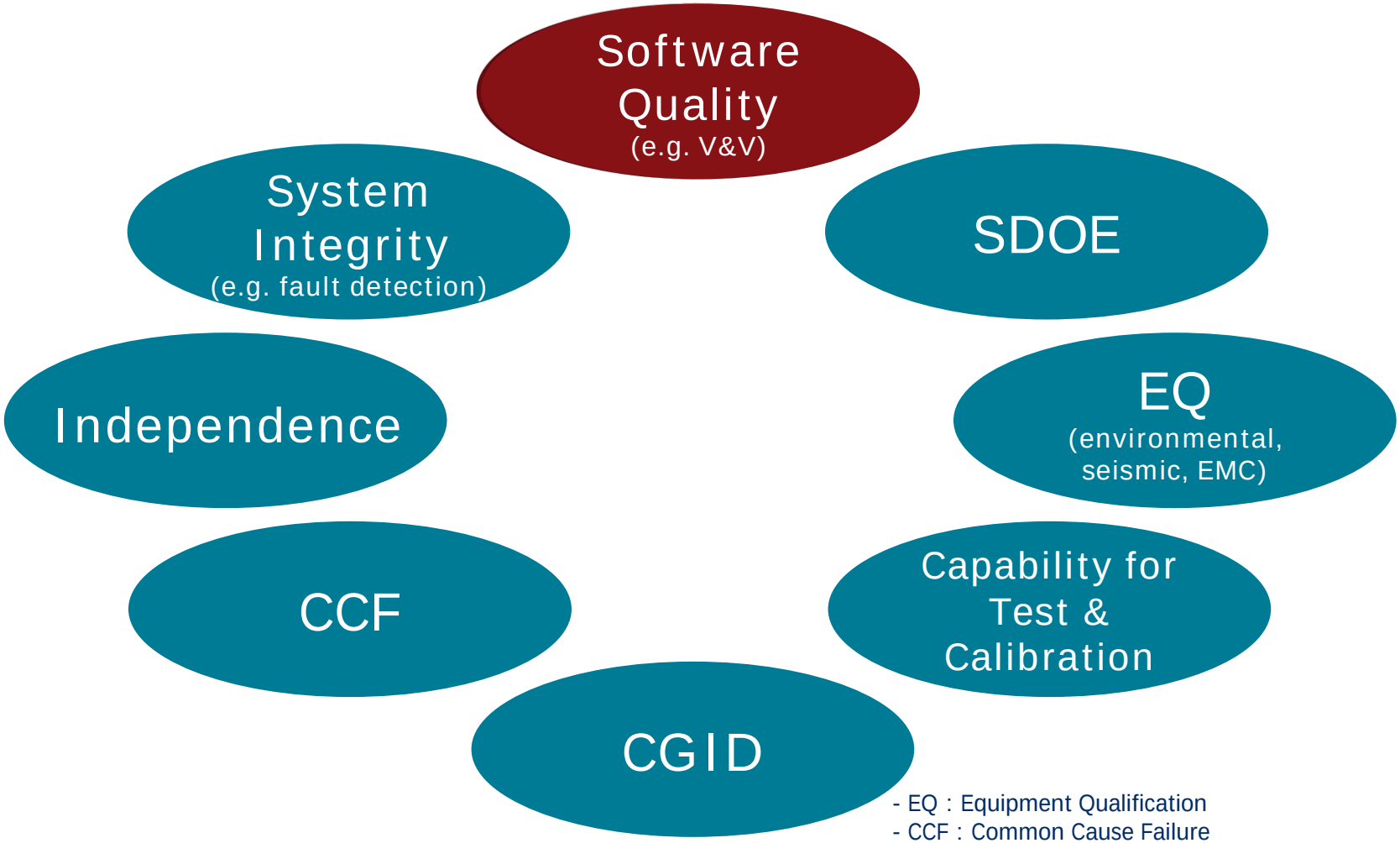
In operation

24 Units
(23,929 MW)

Under construction

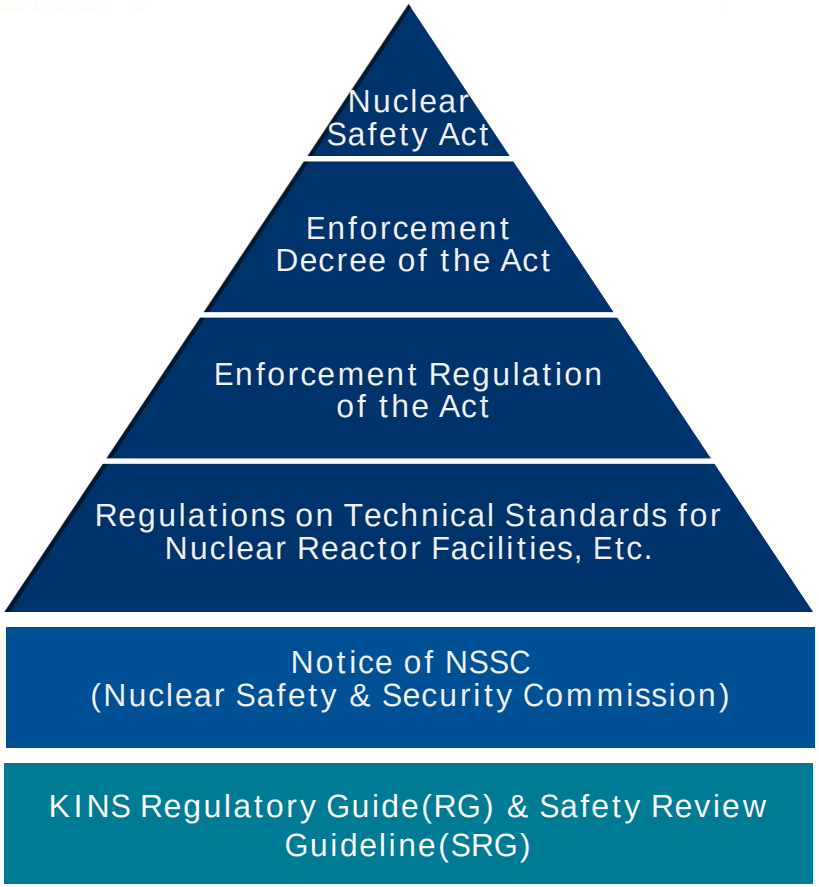
4 Units
(5,600 MW)

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 8.29	• Use of FPGA/CPLD in Safety System • IEC 62566 (partially)
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-05, "Common Position on the Treatment of HDL-programmed Devices for Use in Nuclear Safety Systems", 2013

Review of Software Quality (1/2)

◆ 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						

Review of Software Quality (2/2)

◆ IEEE Std. 1012-2004, "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	Ch. 6, "HPD Requirements Specification"
Design	• Design Specification & Evaluation	• IEEE Std. 7-4.3.2 • IEEE Std. 829 • IEEE Std. 1008	Ch. 8, "HPD Design & Implementation"
Implement., Integration	• Source Code & Evaluation • Component Test Execution		Ch. 9, "HPD Verification"
	• S/W & H/W Integration • Integration Test Execution	• IEEE Std. 7-4.3.2 • IEEE Std. 829	Ch. 10, "HPD aspects of System Integration"
Validation (Test)	• System Test Execution		Ch. 11, "HPD aspects of System Validation"
	• Acceptance Test Execution		Ch. 13, "HPD Production"

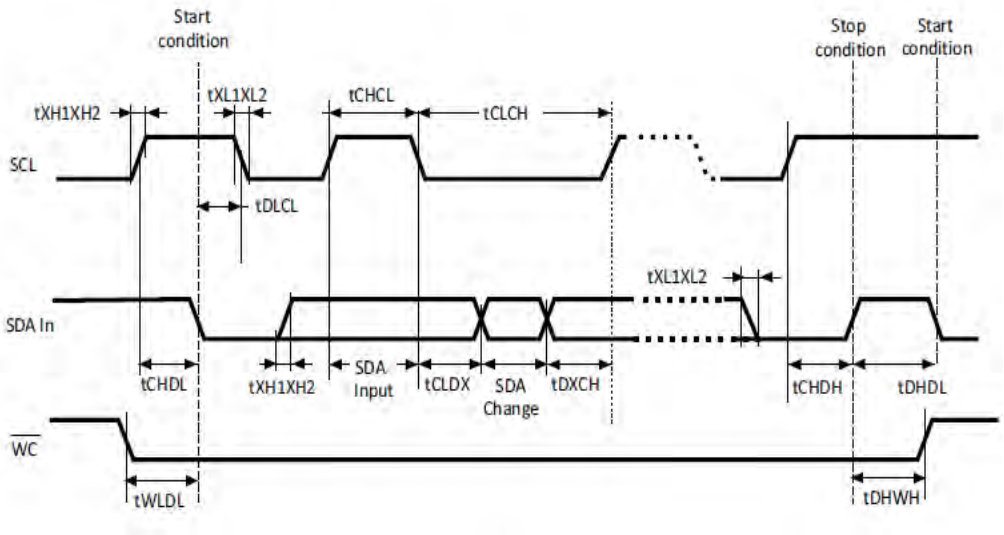
Use of IEC 62566 (2/2)

- 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.

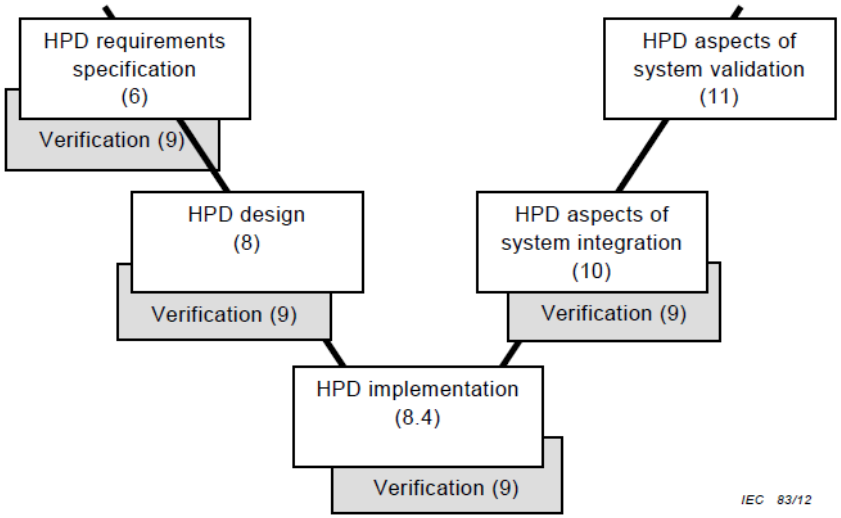
Other Topics of IEC 62566	Existing Standards for Digital I&C Systems
S/W Life Cycle Process (Ch. 5)	• IEEE Std. 1074
S/W QA Plan (Ch. 5)	• IEEE Std. 730
S/W CM Plan (Ch. 5)	• IEEE Std. 828
CGID (Ch. 7)	• EPRI TR-106439, 3002002982 • NRC RG 1.164
S/W Tool Qualification (Ch. 15)	• IEEE Std. 7-4.3.2
CCF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

KINS Reg. Guide 8.29 (1/2)

- A requirement specification shall be written in accordance with IEEE Std. 830 and IEC 62566 Ch. 6.
- 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
- They will be used as acceptance criteria for the validation test.



< Interface Profiles of I²C Bus(EEPROM) >



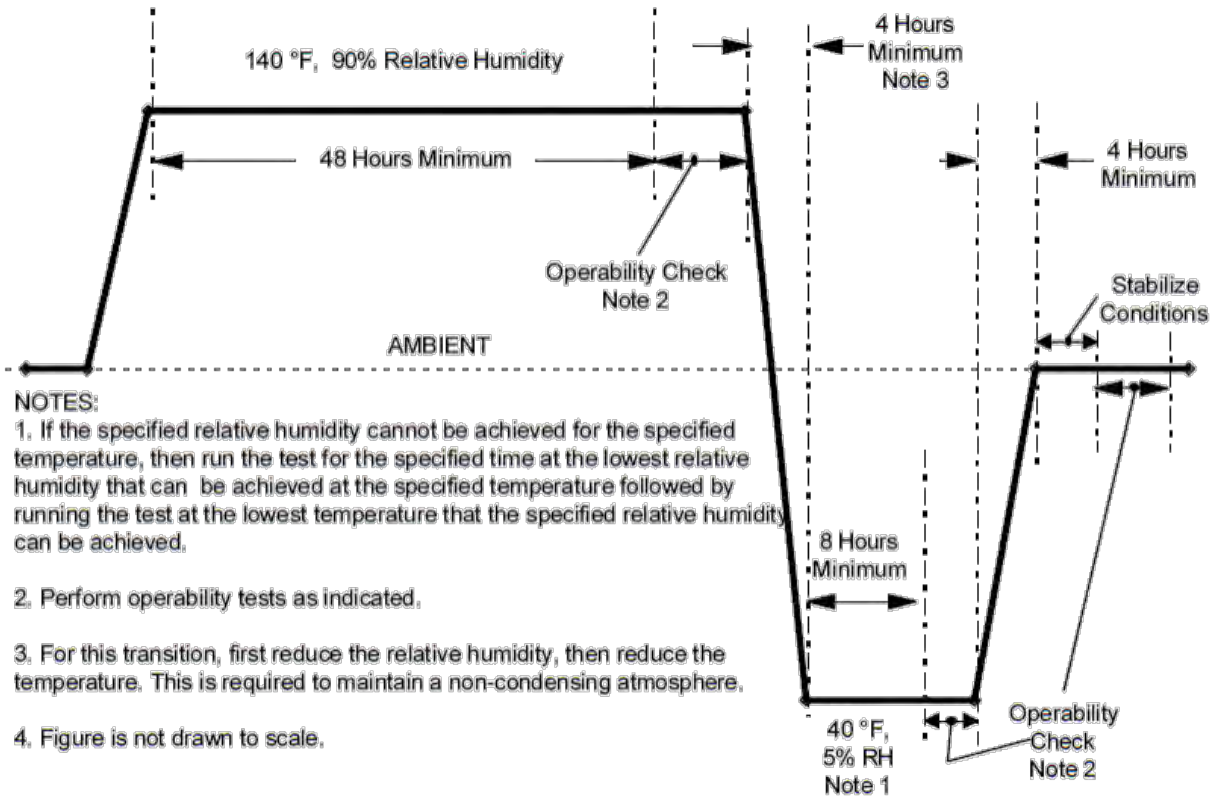
< Development Life Cycle : V Model >

KINS Reg. Guide 8.29 (2/2)

- The FPGA shall be designed/implemented/integrated in compliance with IEC 62566 Ch. 8 and Ch. 10.
- The unit test shall be conducted to meet the requirements of IEC 62566 Ch. 8 and Ch. 9.
- The test-bench for functional simulation of RTL code should have 100% code coverages for statement, branch, expression(condition) and FSM. If not, the documented justification shall be produced.
- The integration/system/acceptance test shall be carried out by IEC 62566 Ch. 10, Ch. 11 and Ch. 13, respectively.

Regulatory Positions (1/2)

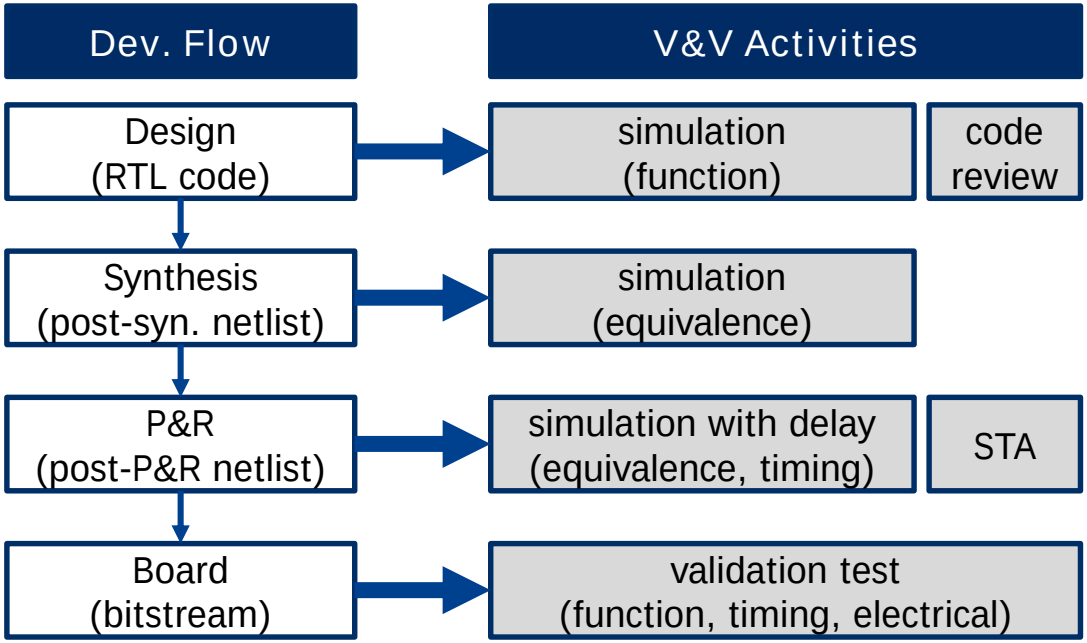
- To ensure the timing constraints are practically met, the type test shall be performed for normal and abnormal service conditions(e.g. temperature, supply voltage) in accordance with IEEE Std. 323.



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

Regulatory Positions (2/2)

- Although there's no HDL code revision, the change in pin allocation or constraints(e.g., timing, fan-out) results in the different result of P&R.
- If they are changed, V&V activities for the affected design shall be carried out.
- The type test should be conducted again to verify the integrity of the revised design within the service conditions such as temperature and supply voltage.



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

< FPGA Development Flow and V&V >

Under Review: DFLC-Q(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(TR)
  - ▷2 stages : "planning ~ requirement" and "design ~ validation"
- Current Status of Review for the 1st TR (~ Oct. 2019)
  - ▷Reviewing the adequacy of the following documents
    - topical report, 12 planning documents, requirement specification
    - safety analysis, V&V and CM reports, etc.

Review for the TR (1/2)

- V&V(Verification & Validation)
  - ▷ The SRS(Software Requirement Specification) shall be evaluated according to the criteria(e.g., accuracy, functionality, reliability, robustness, correctness, consistency, completeness) described in NRC SRP BTP 7-14 and IEEE Std. 1012.
  - ▷ A two-way trace shall exist between each requirement in the SRS and system requirements/design. Undocumented functionality in system documents shall not be introduced to the SRS.
- CM(Configuration Management)
  - ▷ All documents shall be uniquely identified as configuration items.
  - ▷ Configuration control activities such as requesting changes, evaluating changes and approving changes shall be carried out in accordance with IEEE Std. 828.
  - ▷ Configuration items and their information(e.g., publish date, revision #, reviewer) shall be recorded in CM tools and reported to the configuration control board.

Review for the TR (2/2)

- SA(Safety Analysis, IEEE Std. 1228)
  - ▷ A preliminary hazard analysis shall be carried out in the planning phase.
  - ▷ The preliminary hazard list was produced from system requirements and design. And for each hazard, its cause and effect were analyzed.
  - ▷ It should be evaluated that how the hazards can be detected and mitigated by software requirements.
  - ▷ Recommendations from the SA shall be reflected to the SRS and system test plan.
- SDOE(Secure Development and Operational Environment, NRC Reg. Guide 1.152)
  - ▷ In the planning phase, the licensee shall assess the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems that could degrade its reliable operation.
  - ▷ Physical and technical security controls were derived from the assessment.
  - ▷ The software-related security controls(e.g., encryption) were described in the SRS.

Summary

- Introduce the Korean legal system for nuclear safety regulation and international standards/reports used for reviewing S/W quality.
- Activities to confirm S/W quality are totally different between micro-processor and FPGA systems because FPGA is originally hardware. We needed the supplementary requirements suitable for FPGA V&V review.
- Therefore we published KINS Reg. Guide 8.29 that endorses only FPGA-specific parts of IEC 62566 because of the possibility of conflict between IEEE and IEC requirements.
- Present KINS regulatory positions about the type tests carried out after FPGA design changes.
- Talk about KINS review experience in reviewing the FPGA-based controller(DFLC).

Q&A, Comment

KINS
KOREA INSTITUTE OF NUCLEAR SAFETY