I&C for Plant Protection Systems (Regulatory Requirements, Guides, and Standards)

2013 IAEA/ANSN ETTG Workshop on
Nuclear Safety Tailored for Regulators
(17~21 June, 2013)
Int. Nuclear Safety School, KINS, Korea

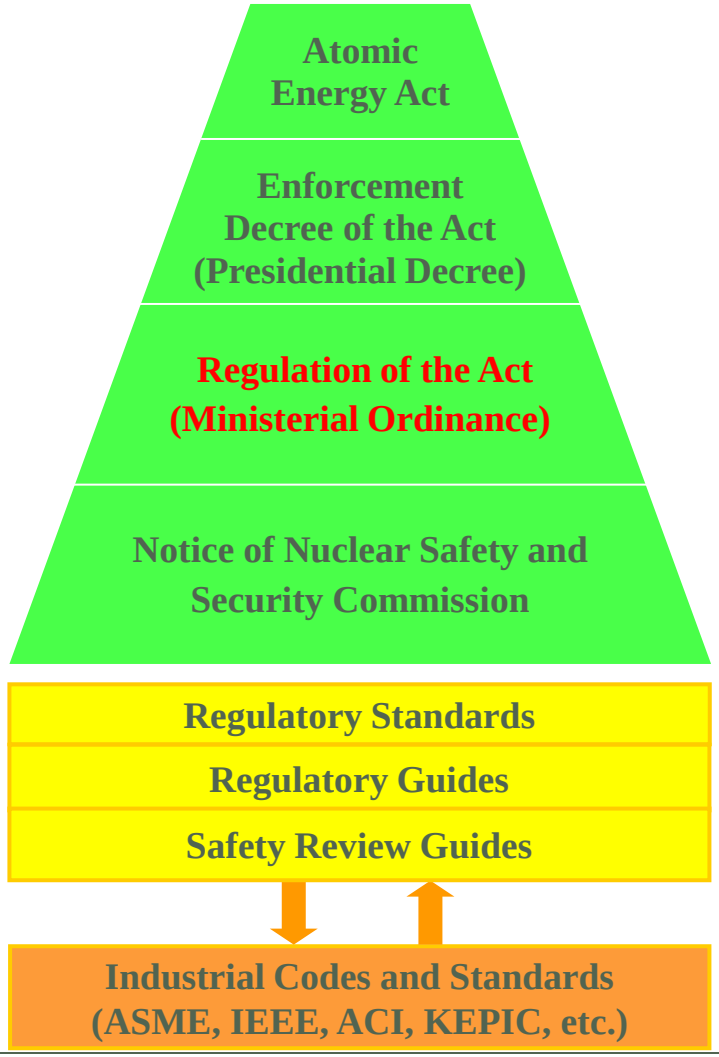
Name : Kim, Bok Ryul
E-mail : k060kbr@kins.re.kr

한국원자력안전기술원
KOREA INSTITUTE OF NUCLEAR SAFETY

CONTENTS

1. Nuclear Regulation and Standards in Korea

Nuclear Regulation and Standards System in Korea

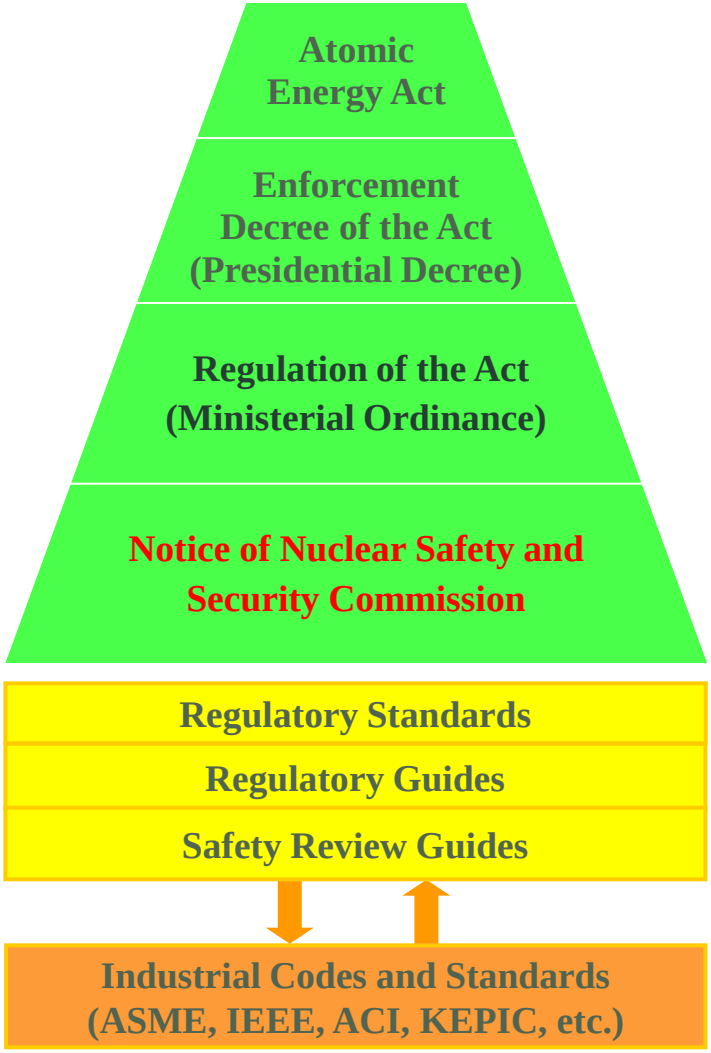


- The Act provides the bases and fundamental matters regarding the development and utilization of nuclear energy and safety regulations
- The Decree provides particulars entrusted by the Act and necessary for the enforcement of the Act
- The Regulation provides the technical standards and particulars entrusted by the Act and the Decree such as detailed procedures and format of documents
- The Notice provides detailed particulars for the technical standards and guidelines
- The Regulatory Standards and Guides provide the interpretation, detailed criteria, acceptable methods, conditions, and specifications of the technical standards.
- The Safety Review Guides provides the staff guidance in carrying out regulatory activities.
- Codes and Standards for materials, design, test, and inspection of components and equipment

Regulations on Technical Standards for Reactor Protection Systems

No.	Title	Equivalency to US 10CFR50, APP. A	Remarks
Article 12	Safety Classes and Standards	GDC 1	
Article 13	External Events Design Bases	GDC 2	
Article 15	Environmental Effects Design Bases, etc	GDC 4	
Article 16	Sharing of Structures, Systems, Components	GDC 5	
Article 20	Instrumentation and Control Systems	GDC 13	
Article 25	Control Room, etc.	GDC 19	
Article 26	Protection System	GDC 20 - 25	
Article 27	Diverse Protection System	GDC 24	
Article 38	Alarm Devices, etc.	GDC 19	

Nuclear Regulation and Standards System in Korea



- The Act provides the bases and fundamental matters regarding the development and utilization of nuclear energy and safety regulations

- The Decree provides particulars entrusted by the Act and necessary for the enforcement of the Act

- The Regulation provides the technical standards and particulars entrusted by the Act and the Decree such as detailed procedures and format of documents

- The Notice provides detailed particulars for the technical standards and guidelines

- The Regulatory Standards and Guides provide the interpretation, detailed criteria, acceptable methods, conditions, and specifications of the technical standards.
- The Safety Review Guides provides the staff guidance in carrying out regulatory activities.

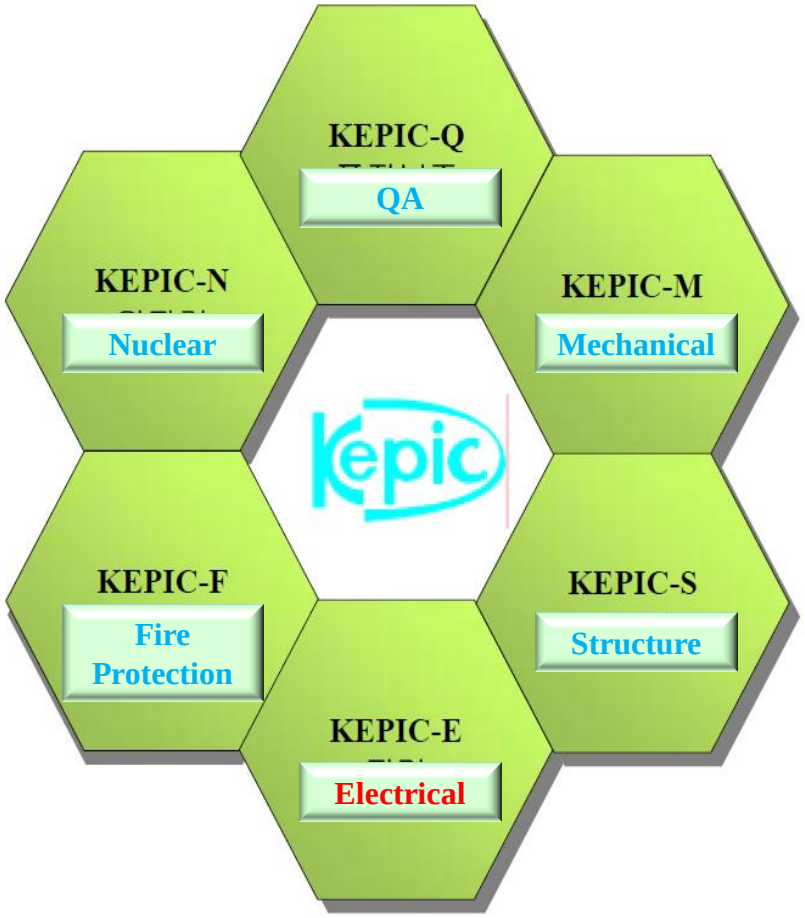
- Codes and Standards for materials, design, test, and inspection of components and equipment

Structure of KEPIC Code

- Q(Quality), M(Mechanical), E(Electrical), S(Structure), F(Fire), N(Nuclear)

- EN(Electrical Nuclear)
  EM(Electrical Measurement
  EE(Electrical Equipment)
  EC(Electrical Cable)
  ET(Electrical Transmitter)

- ENA: General
  ENB/D: Design/Qualification
  ENE: Installation
  ENF: Testing and Inspectio

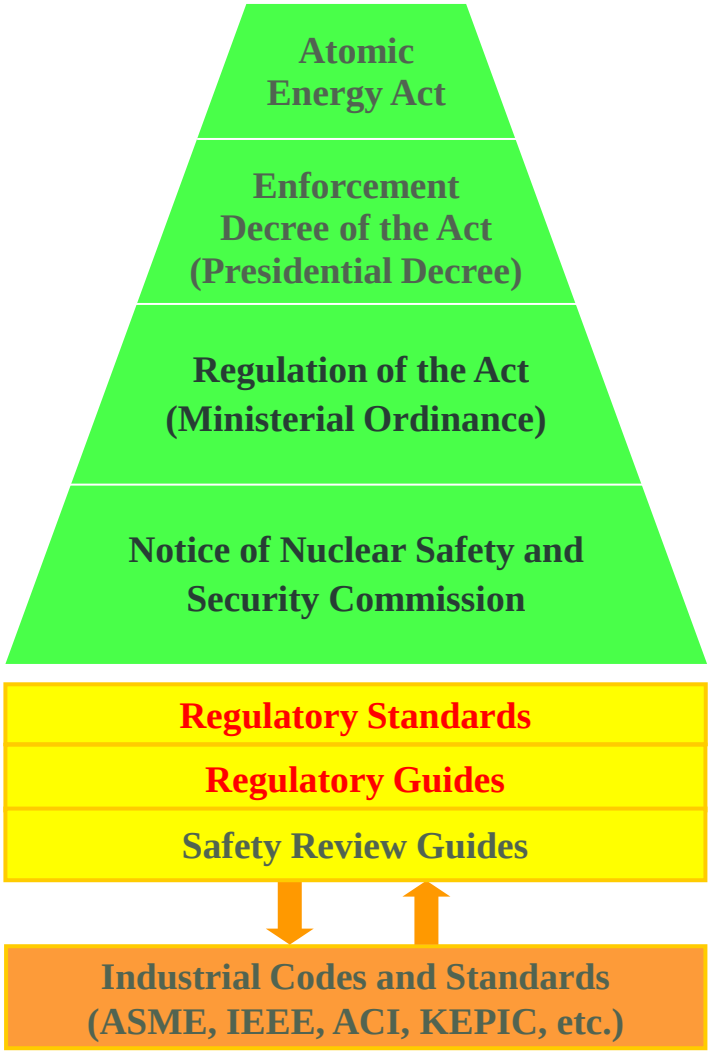


Notice of Nuclear Safety and Security Commission

The Notice of NSSC No.2010-28, "Guidelines for Application of Korea Electric Power Industry Code (KEPIC) as Technical Standards of Nuclear Reactor Facilities" approves the following KEPIC codes.

KEPIC	IEEE/ANS/ISA	Remarks
ENA	ANSI/ANS 51.1-1983 (R1988)	General
ENB	IEEE 279(R78), 308('01), 317 ('96), 352('87, R99), 379('94, '00), 384('92, R97), 387('01), 420('01), 494('74, R90), 497('02), 577('04), 603('98), 741('02), 765('06), 946('04), 7-4.3.2('03), ANSI/ISA S67.04.01 ('94, '00)	Design
END	IEEE 323('83, R96, '03), 334('99), 344('87, '04), 382('96), 383('74, '03), 535('94), 572('92), 627('80, R96), 649('99), 650('06)	Qualification
ENE	IEEE 336('91), 628('01), 690('02), ANSI/ISA S67.01('94)	Installation
ENF	IEEE 336('91), 338('87, R2000)	Test and Inspection
EMC	IEEE 1050('99)	Grounding

Nuclear Regulation and Standards System in Korea



- The Act provides the bases and fundamental matters regarding the development and utilization of nuclear energy and safety regulations
- The Decree provides particulars entrusted by the Act and necessary for the enforcement of the Act
- The Regulation provides the technical standards and particulars entrusted by the Act and the Decree such as detailed procedures and format of documents
- The Notice provides detailed particulars for the technical standards and guidelines
- The Regulatory Standards and Guides provide the interpretation, detailed criteria, acceptable methods, conditions, and specifications of the technical standards.
- The Safety Review Guides provides the staff guidance in carrying out regulatory activities.
- Codes and Standards for materials, design, test, and inspection of components and equipment

Regulatory Standards for I&C Systems (KINS/RS-N08.00)

Section	Subsection	Title	Remarks
8.1		Overview	
	8.1.1	Objectives	
	8.1.2	Definitions	
8.2		Reactor Protection System	
	8.2.1	Application Scope	
	8.2.2	Design Bases	
	8.2.3	General Functions and Reliability	
	8.2.4	Single Failure Criterion	
	8.2.5	Completion of Protective Actions	
	8.2.6	Automatic and Manual Controls	
	8.2.7	Quality Assurance	
	8.2.8	Equipment Qualification	
	8.2.9	System Integrity	

Regulatory Standards for I&C Systems (KINS/RS-N08.00)

Section	Subsection	Title	Remarks
8.2	8.2.10	Independence	
	8.2.11	Common Cause Failures and Diversity	
	8.2.12	Derivation of System Input Signals	
	8.2.13	Test and Calibration	
	8.2.14	Operating Bypasses	
	8.2.15	Maintenance Bypasses	
	8.2.16	Indication of Bypass Functions	
	8.2.17	Set Points	
	8.2.18	Access Control	
	8.2.19	Information Display	
	8.2.20	Maintainability	
	8.2.21	Identification	
	8.2.22-23	Requirements of Power sources and Auxiliary Systems	

Regulatory Standards for I&C Systems (KINS/RS-N08.00)

Section	Subsection	Title	Remarks
8.3		Safety-Related I&C Systems	
	8.3.1	Application Scope	
	8.3.2	Design Bases	
	8.3.3	General Functions and Reliability	
	8.3.4	Single Failure Criterion	
	8.3.5	Completion of Safety-Related Actions	
	8.3.6	Automatic and Manual Controls	
	8.3.7	Quality Assurance	
	8.3.8	Equipment Qualification	
	8.3.9	System Integrity	
	8.3.10	Independence	
	8.3.11	Test and Calibration	
	8.3.12	Set Points	

Regulatory Standards for I&C Systems (KINS/RS-N08.00)

Section	Subsection	Title	Remarks
	8.3.13	Access Control	
	8.3.14	Maintainability	
	8.3.15	Identification	
	8.3.16	Requirements of Power sources	
	8.3.17	Requirements of Auxiliary Systems	
	8.3.18	I&C System for Safe Shutdown	
	8.3.19	Safety-Related Information Systems	
	8.3.20	Safety-Related Interlock Systems	
	8.3.21	Reactor Control Room	
	8.3.22	Remote Shutdown Room	

Regulatory Standards for I&C Systems (KINS/RS-N08.00)

Section	Subsection	Title	Remarks
8.4		Diverse I&C Systems	
	8.4.1	Application Scope	
	8.4.2	Design Bases	
	8.4.3	General Functions and Reliability	
	8.4.4	Completion of Diverse Protective Actions	
	8.4.5	Quality Assurance	
	8.4.6	Equipment Qualification	
	8.4.7	Independence	
	8.4.8	Defense-in-Depth and Diversity	
	8.4.9	Test and Maintainability	
	8.4.10	Access Control	
	8.4.11	Information Displays	
	8.4.12-13	Requirements of Power sources and Auxiliary Systems	

Regulatory Guides for I&C Systems (KINS/RG-N08.00)

No.	Title	Equivalency to NRC RG	Remarks
KINS/RG-N08.01	Safety Classifications of I&C Systems	None	
KINS/RG-N08.02	Periodic Testing for Actuation Functions of Safety Systems	RG 1.22	
KINS/RG-N08.03	Quality Assurance for Installation, Inspection and Testing of I&C and Electric Facilities	RG 1.30	
KINS/RG-N08.04	Bypassed and Inoperable Status Indication for Safety Systems	RG 1.47	
KINS/RG-N08.05	Application of Single Failure Criterion to Safety Systems	RG 1.53	
KINS/RG-N08.06	Manual Initiation of Protective Actions	RG 1.62	
KINS/RG-N08.07	Initial Startup Test Program to Demonstrate Remote Shutdown Capability	RG 1.68.2	
KINS/RG-N08.08	Instrumentation for Monitoring Plant Status During and Following an Accident	RG 1.97	

Regulatory Guides for I&C Systems (KINS/RG-N08.00)

No.	Title	Equivalency to NRC RG	Remarks
KINS/RG-N08.09	Set Points for Safety-Related Instrumentation	RG 1.105	
KINS/RG-N08.10	Periodic Testing for Electric Power and Protection Systems	RG 1.118	
KINS/RG-N08.11	Loose-Part Detection Program for Primary System	RG 1.133	
KINS/RG-N08.12	Instrument Sensing Lines	RG 1.151	
KINS/RG-N08.13	Use of Digital Computers in Safety Systems	RG 1.152	
KINS/RG-N08.14	Design of Safety Class I&C Systems	RG 1.153	
KINS/RG-N08.15	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems	RG 1.168	
KINS/RG-N08.16	Configuration Management Plans for Digital Computer Software Used in Safety Systems	RG 1.169	

Regulatory Guides for I&C Systems (KINS/RG-N08.00)

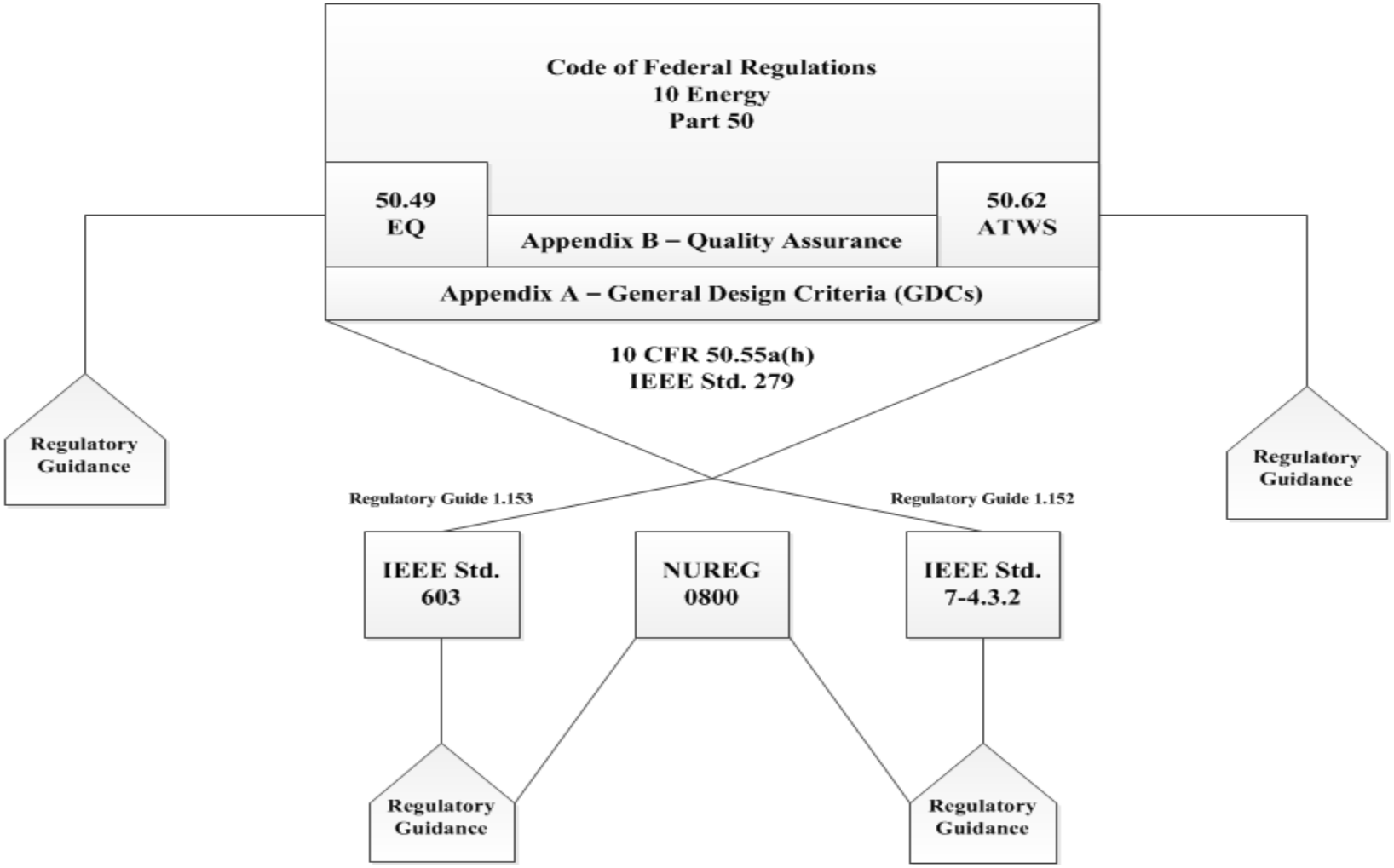
No.	Title	Equivalency to NRC RG	Remarks
KINS/RG-N08.17	Software Test Documentation for Digital Computer Software Used in Safety Systems	RG 1.170	
KINS/RG-N08.18	Software Unit Testing for Digital Computer Software Used in Safety Systems	RG 1.171	
KINS/RG-N08.19	Software Requirements Specifications for Digital Computer Software Used in Safety Systems	RG 1.172	
KINS/RG-N08.20	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems	RG 1.173	
KINS/RG-N08.21	Display and Alarms for Control Room Information	None	
KINS/RG-N08.22	Cyber Security for I&C Systems	None	
KINS/RG-N08.23	Real-Time Evaluation of Digital I&C System	None	

Regulatory Guides for I&C Systems (KINS/RG-N08.00)

No.	Title	Equivalency to NRC RG	Remarks
KINS/RG-N08.24	Reviews of Safety Software – Software Life Cycle Process Plans	None	
KINS/RG-N08.25	Reviews of Safety Software – Implementation for Software Life Cycle Processes	None	
KINS/RG-N08.26	Reviews of Safety Software – Design Results for Software Life Cycle Processes	None	
KINS/RG-N08.27	Software Safety Hazards Analysis	None	
KINS/RG-N08.28	Independence for Data Communications	None	

2. Nuclear Regulation and Standards in USA

Nuclear Regulation and Standards for Reactor Protection System (1/2)



Nuclear Regulation and Standards for Reactor Protection System (2/2)

- The I&C review information is presented in 3 segments.
  - A description and review of the 10 CFR 50 Appendix A *General Design Criterion(GDC)* essential to the I&C review
  - A description of the *Environmental Qualification Rule* and the *ATWS Rule* included in 10 CFR 50
  - An explanation of *10 CFR 50.55a subpart (h)* and the purpose of IEEE Standards 279 and 603

Examples of Applying GDC to Protection Systems (1/4)

GDC 20 – Protection System Functions

– The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

❖ Equivalent to Article 26(Reactor protection System) of Regulation on Technical Standards in Korea

– *Applicability* :

- Reactor Trip system
- Engineered Safety Features Actuation System

Examples of Applying GDC to Protection Systems (2/4)

GDC 20 – Protection System Functions

- The I&C licensing reviewer verifies that:
  - The protection system is designed to automatically initiate appropriate systems including reactivity control to assure that fuel design limits are not exceeded as a result of anticipated operational occurrences.
  - The protection system is designed to sense accident conditions and to initiate the operation of systems and components important to safety.

Examples of Applying GDC to Protection Systems (3/4)

GDC 22 – Protection System Independence

- The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to extent practical to prevent loss of the protection function.

❖ Equivalent to Article 26(Reactor Protection System) of Regulation on Technical Standards in Korea

- *Applicability* :
  - Reactor Trip system
  - Engineered Safety Features Actuation System

Examples of Applying GDC to Protection Systems (4/4)

- **GDC 22 – Protection System Independence**
  - The I&C licensing reviewer verifies that:
    - The protection system design assures that the effects of the following on redundant channels do not result in the loss of a protective function.
      - Natural phenomena
      - Normal operating conditions
      - Maintenance activity
      - Testing activity
      - Postulated accident conditions
    - Functional diversity is incorporated to the extent practicable to prevent loss of function.
    - Diversity in component design is incorporated to the extent practicable to prevent loss of function.

10 CFR 50.49 and 10 CFR 50.62 (1/3)

Needs of Establishing 10 CFR 50.49 and 50.62

- Concerns in 1970' about Common Mode Failures prompted additional regulations to deal with Environmental Qualification and ATWS.
- Adverse environments (steam, temperature, radiation) could cause common mode failures in RPS and ESFAS.
  - *USNRC addressed this issue by requiring improved design margins and qualification testing.*
- Uncertainties in the Reactor Protection System reliability due to potential of common mode failures lead to need for diversity
  - *USNRC addressed this issue by requiring diversity as well as redundancy in Reactor Protection System.*

10 CFR 50.49 and 10 CFR 50.62 (2/3)

- **10 CFR 50.49 "Environmental Qualification of Electrical Equipment Important to Safety for Nuclear Power Plants"**
  - Became enforceable law January 21, 1983
  - Establishes specific requirements for the environmental qualification of electrical equipment in systems important to safety
  - Requires an established program
  - Amplifies requirements of 10 CFR 50 Appendix A, General Design Criterion 2 and 4
  - ❖ Equivalent to Article 24(Details of Periodic Safety Reviews) of Enforcement Regulation in Korea

10 CFR 50.49 and 10 CFR 50.62 (3/3)

- **10 CFR 50.62 "Requirements for Reduction of Risk from Anticipated Transients Without Scram(ATWS) Events for Nuclear Power Plants"**
  - Became enforceable law June 26, 1984
  - Establishes specific requirements for pressurized water reactors and boiling water reactors
  - Established the following requirements for pressurized water reactor(PWR)
    - Each PWR must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary feedwater system and initiate a turbine trip under conditions indicative of an ATWS.
  - ❖ Equivalent to Article 27(Diverse Protection System) of Regulation on Technical Standards in Korea

10 CFR 50.55a(h) Codes and Standards

Approval of Codes and Standards

- 10 CFR 50.55a(h) invoked IEEE Std. 603 "Criteria for Protection Systems for Nuclear Power Generating Stations" into law on May 13, 1999.
- The criteria in IEEE Std. 603 are an industry consensus of an acceptable approach to assessing the adequacy of protection system functional performance and reliability in meeting design requirements
- IEEE Std. 279 was based on a "discipline approach" to establishing protection system criteria. IEEE Std. 603 was based on a "system approach" to establishing protection system criteria.

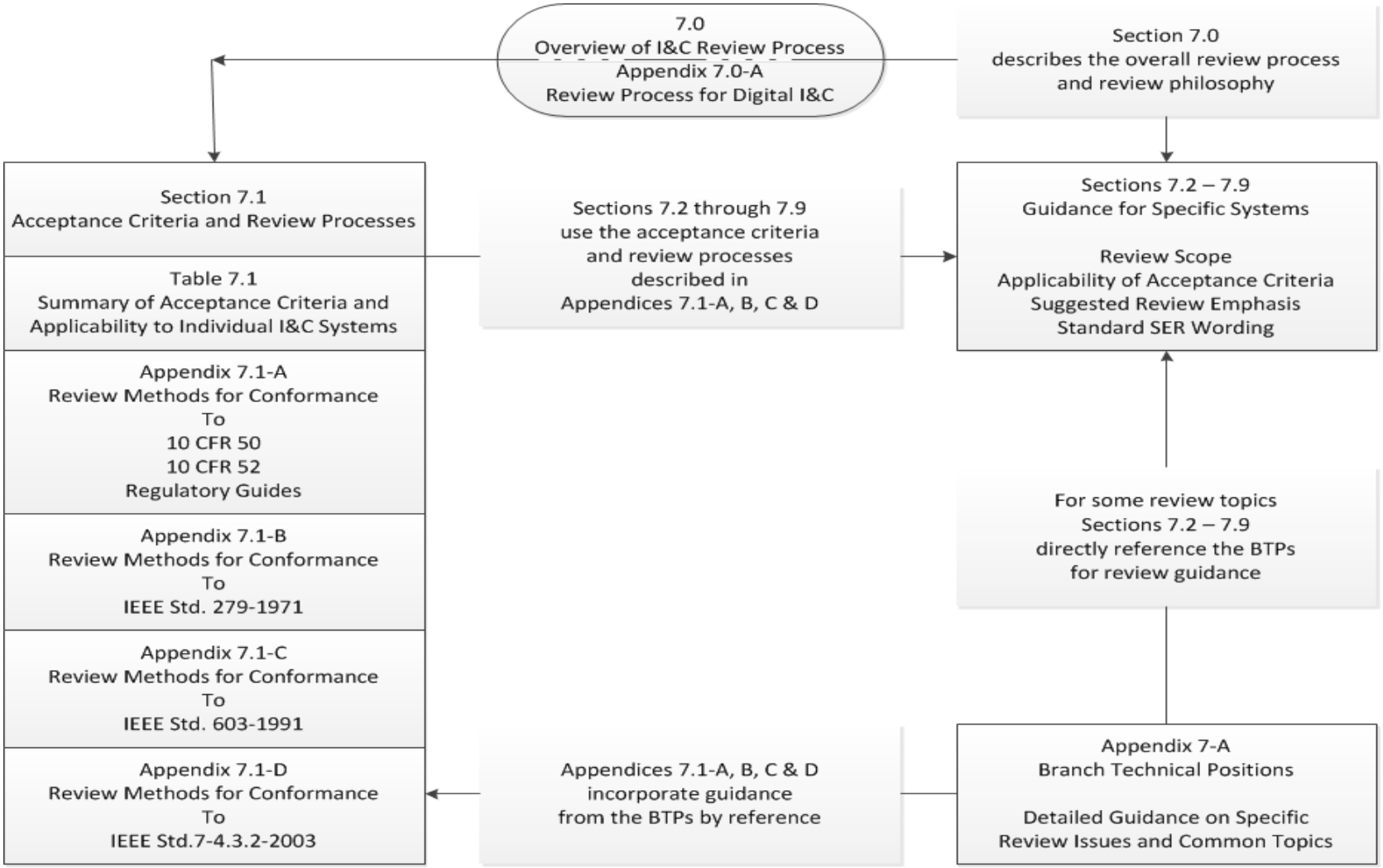
❖ Equivalent to Section 8.2(Reactor Protection System) of Regulatory Standards for I&C Systems in Korea

NUREG-0800 Standard Review Plan (SRP)

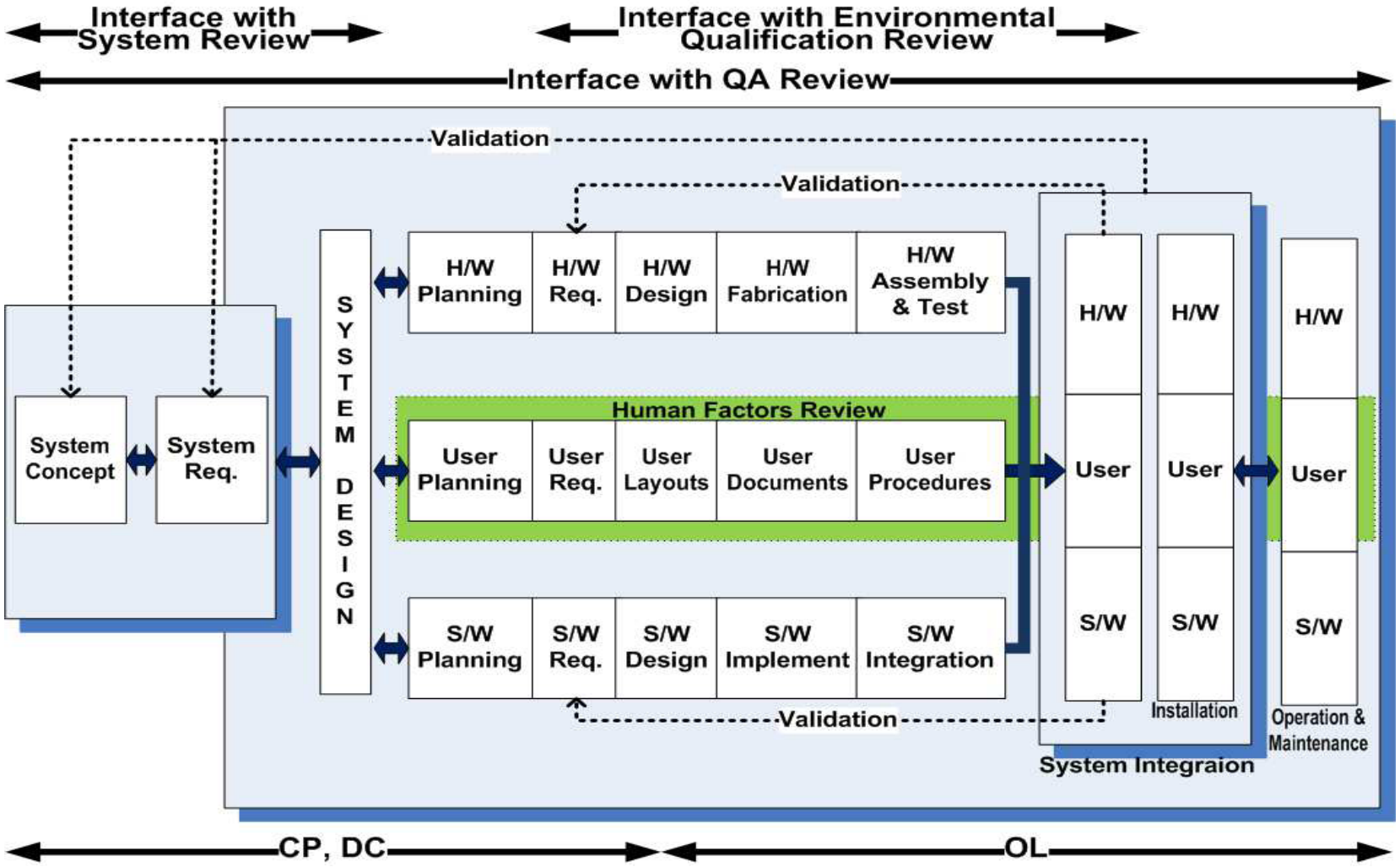
Overview

- Provides Regulatory Guidance only(not enforceable by law)
- Provides guidance based on review of Safety Analysis Reports (SARs)
- Provides guidance in the evaluation of conformance to USNRC regulation
  - Cross discipline review coordination
  - Provides guidance in evaluation of TMI Action Plan requirements
  - Includes guidance for the review of programmable digital system designs

Structure of SRP Chapter 7



Development and Review Processes



Requirements and Acceptance Criteria for I&C Systems (Table 7-1)

	Title	Applicability (SAR/SRP Section)								Remarks
GDC, Appendix A to 10 CFR Part 50		7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
GDC 1	Quality Standards and Records	R	R	R	R	R	R	R	R	Article 12
GDC 2	Design Bases for Protection Against Natural Phenomena	R	R	R	R	R				Article 13
GDC 4	Environmental and Dynamic Effects Design Bases	R	R	R	R	R				Article 15
GDC 10	Reactor Design	R	R			R	R			Article 17
GDC 13	Instrumentation and Control	R	R	R	R	R	R	R		Article 20
GDC 19	Control Room	R	R	R	R	R	R	R		Article 25
GDC 20	Protection System Functions	R	R							Article 26
GDC 21	Protection Systems Reliability and Testability	R	R							Article 26
GDC 22	Protection System Independence	R	R							Article 26
GDC 23	Protection System Failure Modes	R	R							Article 26
GDC 24	Separation of Protection and Control Systems	R	R	R	R	R	R	R	R	Article 26
GDC 25	Requirements for Reactivity Control Malfunctions	R								Article 28

Requirements and Acceptance Criteria for I&C Systems (Table 7-1)

	Title	Applicability (SAR/SRP Section)								Remarks
Staff Requirements Memoranda (SECY 93-087)		7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
II.Q	Defense Against CMFs in Digital I&C Systems	A	A				A	A		Article 26
II.T	Control Room Annunciator (Alarm) Reliability				A					Article 38
Regulatory Guides										
RG 1.22	Periodic Testing of Protection System Actuation Functions	A	A					A		BTP 7-8
RG 1.47	Bypassed and Inoperable Status Indicator for NPP Safety Systems	A	A			A	A			
RG 1.53	Application of the Single-Failure Criterion to Safety Systems	A	A	A	A	A				IEEE Std. 379-2000
RG 1.62	Manual Initiation of Protective Actions	A	A					A		
RG 1.97	Criteria for Accident Monitoring Instrumentation for NPPs				A					IEEE Std. 497-2002
RG1.105	Setpoints for Safety-Related Instrumentation	A	A	A	A	A	A	A	A	ISA S67.04-1994
RG1.118	Periodic Testing of Electric Power and Protection Systems	A	A	A	A	A		A		IEEE Std. 338-1987

Requirements and Acceptance Criteria for I&C Systems (Table 7-1)

	Title	Applicability (SAR/SRP Section)								Remarks
Regulatory Guides		7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
RG1.151	Instrument Sensing Lines	A	A	A	A	A	A	A		ISA-S67.02
RG1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	A	A	A	A	A	A	A	A	IEEE Std. 7-4.3.2-2003
RG1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of NPPs	A	A	A	A	A	A	A	A	IEEE Std. 1012-1998
RG1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of NPPs	A	A	A	A	A	A	A	A	IEEE Std. 828-1983
RG1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of NPPs	A	A	A	A	A	A	A	A	IEEE Std. 829-1983
RG1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of NPPs	A	A	A	A	A	A	A	A	IEEE Std. 1008-1987
RG1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of NPPs	A	A	A	A	A	A	A	A	IEEE Std. 830-1993

3. Nuclear Regulation and Standards for Digital I&C Systems

Relationship between IEEE 603 and 7-4.3.2 (1/5)

Overview

- IEEE Std. 603-1998 establishes the minimum functional design criteria for:
  - The instrumentation portion of safety systems
  - The control portions of safety systems
  - The power portion of safety systems
- IEEE Std. 603-1998 does not directly discuss digital systems.
- The guidance on the application of the criteria in IEEE Std. 603-1998 for safety systems using digital programmable computers is provided in IEEE Std. 7-4.3.2-2003.
- IEEE Std. 7-4.3.2-2003 specifies computer-specific criteria (incorporating hardware, software, firmware, and interfaces) to supplement the criteria in IEEE Std. 603-1998.

Relationship between IEEE 603 and 7-4.3.2 (2/5)

Mapping of IEEE 603-1998 to IEEE 7-4.3.2-2003

IEEE Std. 603-1998 Criteria	IEEE Std. 7-4.3.2-2003 Additional Requirements	Annex for Guidance
4. Safety system design basis	Safety system design basis	Annex B
5. Safety system criteria	None	Annex B
5.1 Single failure criterion	None	-
5.2 Completion of protective action	None	-
5.3 Quality	5.3.1 Software development 5.3.2 Software tools 5.3.3 Verification and validation 5.3.4 Independent V&V 5.3.5 Software configuration management 5.3.6 Software project risk management	Annex D and Annex F

Relationship between IEEE 603 and 7-4.3.2 (3/5)

Mapping of IEEE 603-1998 to IEEE 7-4.3.2-2003

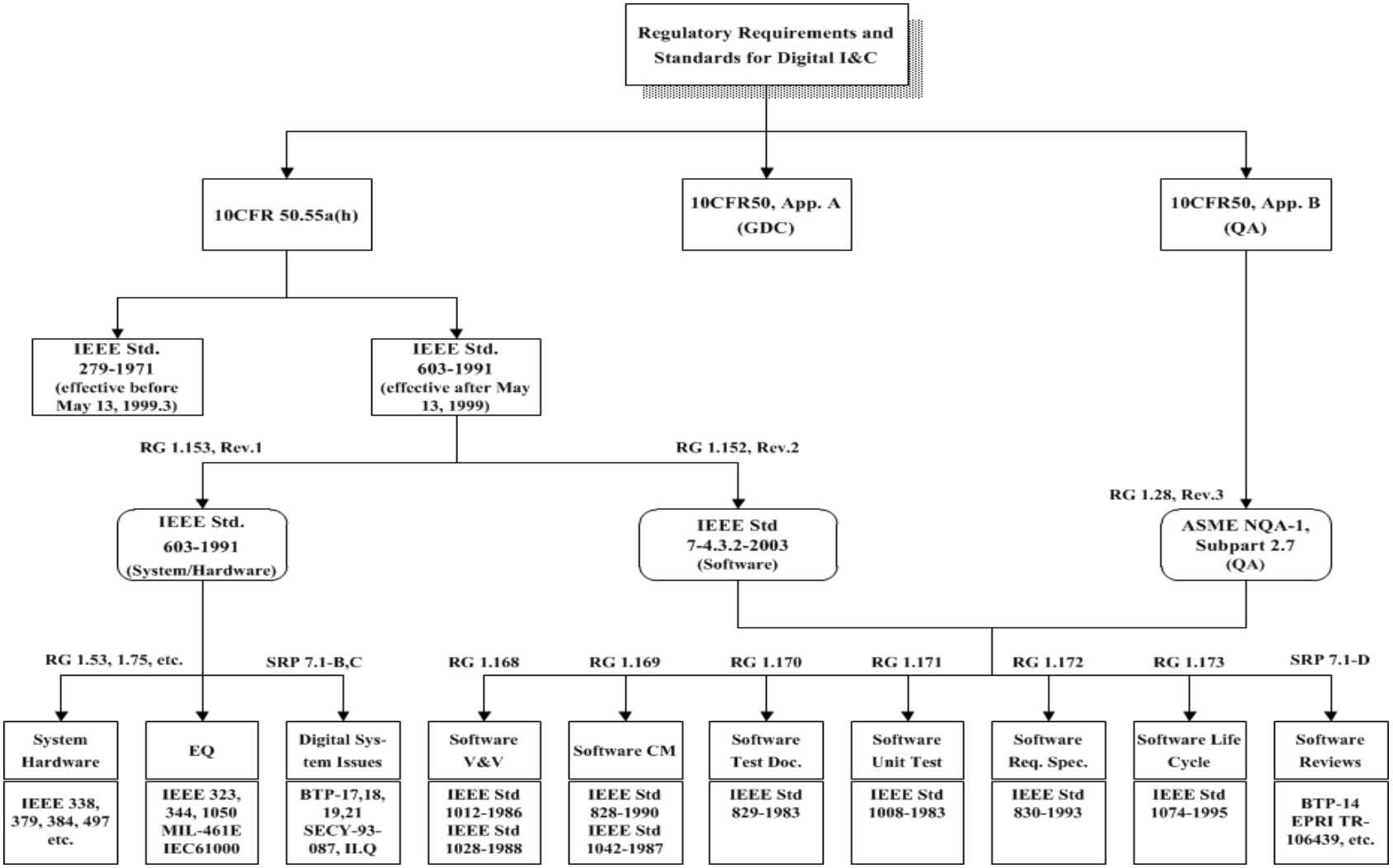
IEEE Std. 603-1998 Criteria	IEEE Std. 7-4.3.2-2003 Additional Requirements	Annex for Guidance
5.4 Equipment qualification	5.4.1 Testing software and diagnostics 5.4.2 Qualification of existing commercial computers	Annex C
5.5 System integrity	5.5.1 Design for computer integrity 5.5.2 Design for test & calibration 5.5.3 Fault detection and self-diagnostics	Annex B and Annex C
5.6 Independence	5.6 Independence	Annex E
5.7 Capability for test and calibration	None	-
5.8 Information displays	None	-

Relationship between IEEE 603 and 7-4.3.2 (4/5)

Mapping of IEEE 603-1998 to IEEE 7-4.3.2-2003

IEEE Std. 603-1998 Criteria	IEEE Std. 7-4.3.2-2003 Additional Requirements	Annex for Guidance
5.9 Control of Access	None	-
5.10 Repair	None	-
5.11 Identification	None	-
5.12 Auxiliary features	None	-
5.13 Multi-unit stations	None	-
5.14 Human factor considerations	None	
5.15 Reliability	5.15 Reliability	Annex F

Relationship between IEEE 603 and 7-4.3.2 (5/5)



Always we keep watching our Atomic Power

Name : Kim, Bok Ryul
E-mail : k060kbr@kins.re.kr

Thank You

한국원자력안전기술원
KOREA INSTITUTE OF NUCLEAR SAFETY