Acceptable FPGA Framework based on the IEEE Std-1012 and IEC Std-62566

Oct. 8th , 2018

Jang Yeol Kim

KAERI

KAERI 한국원자력연구원 Korea Atomic Energy Research Institute

– Table of Contents –

The History of V&V

PAST	Present	Future
oTesting oriented V&V oTraceability oSafety & Security Testing	oItem based(Embedded) - SW - SW + HW - Embedded(FPGA) - System oStandardization - USNRC-IEEE Std. - IAEA-IEC Std. o Item based V&V - Sil Level	o Risk based V&V o Vulnerable of AI SW Safety - Need to know Decision Background

Scope of V&V

- Safety-critical(Cat A) Software
  - To develop of Safety-critical SW for delivery to a customer
  - In-house
  - Use of SW for Licensing (Used for regulatory body)
  - COTS Software
- V&V Activities
  - Review
  - Audit
  - Analysis, Testing & Evaluation
  - Software Safety Analysis
  - COTS SW Evaluation
- Exception
  - Administration and Financial oriented SW such as MIS and commercial application software(MS-Office, VISIO etc.)

Assumptions(1)

- The existence of a system requirement specification
  - Complete/Consistent/Unambiguous
- Provide a Hardware view of V&V
- How to setup for Acceptance Framework Criteria
  - Complete/Consistent/Unambiguous
  - Industrial + NPPs FPGA
    - IEEE Std-1012 : Typical
    - IEC Std-62566 : NPPs
  - Nuclear Safety System
    - 10CFR50
    - NUREG/DG-1054 -> RG 1.168
      {Independence/Audit/Configuration Mgt.)
    - IEEE Std-1074 : SWLC, Activity mapping

Assumptions(2)

- Nuclear Safety System
  - IEEE Std-603 : NPP Safety System
  - IEEE Std 7-4.3.2 : HW, SW, I/F Safety System consideration factors
  - NUREG/BTP-14 : Relationship of SVV, SCM, and SSA
  - IEEE Std-1228
    - Software Safety Analysis
  - NUREG/CR-6421 ; COTS SW dedication
    - IEEE Std 7-4.3.2 : Tools Qualification

Before starting V&V

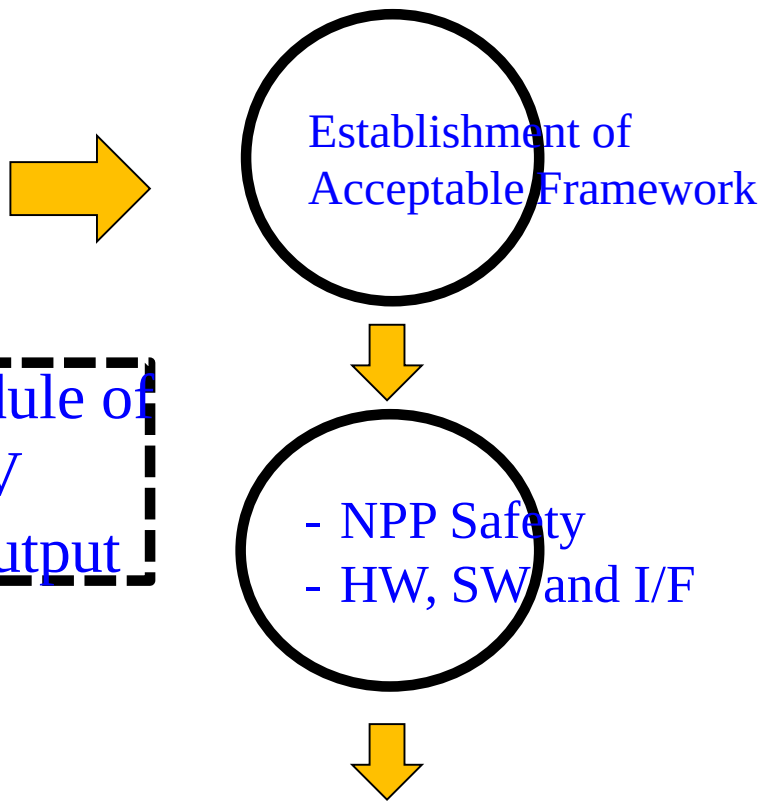
- Preparing of QA Manual / QA Procedure
  - Work flow, Audit/Inspection Plan, Schedule and Date etc.
  - Several Forms
- Establishing of Baseline on Code Cut-off Date
  - Acceptable framework
  - USNRC-based vs IAEA-based
- Terms and Abbreviations for dedicated projects
- Document Deliverable List
  - MS-Excel or Project Management tool
  - Dev. And V&V

Flow of Acceptable Framework

QAM/QAP
Project Mgt. Process

Baseline of
Code Cut-off Date

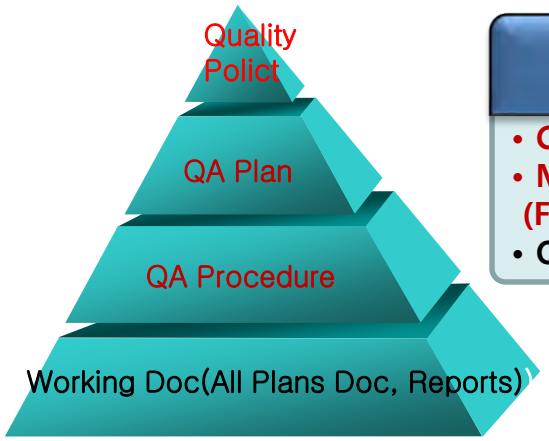
Process Schedule of
Dev. and V&V
for Design Output



SWLC	Applied Code & STD

Quality Assurance Activity

- 10CFR50 Appendix B
  - ASME/NQA-1-2008, Agenda-2009
  - (KEPIC-2011 Appendix Full Revision)



Continuous Improving

Establishment ofQA System
- QA Coordinator
  - All Prj Members
- Operation and Maintenance of QAP/QA Proc.
- Education and Training / Staff Qualification

QA Plan Execution
- Working according to QAP
  - Mg't of Design Doc Preparing/Review/Approval

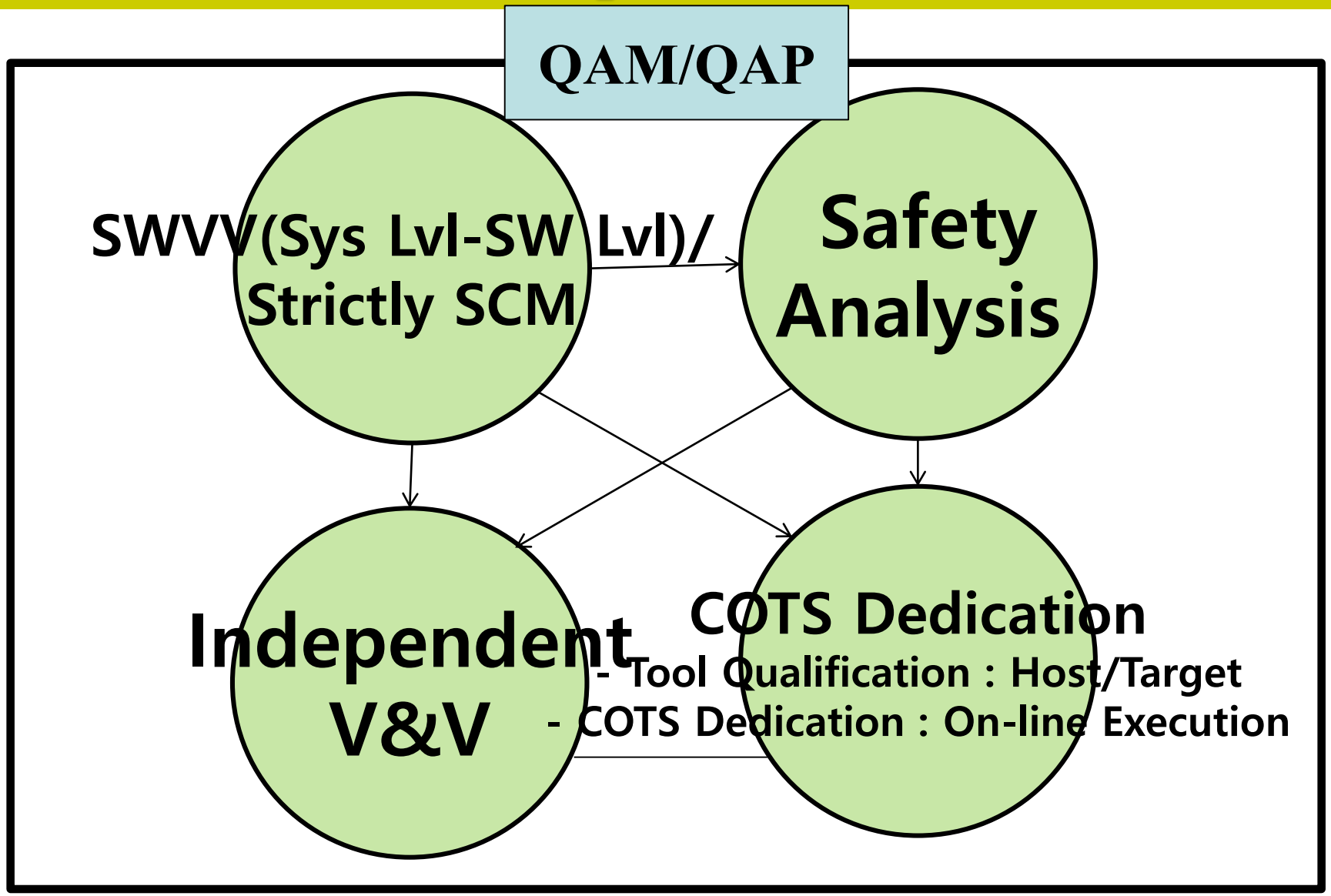
Implementation Audit
- QA Rec. Review
- QA Audit/QA Inspection

CAR and Improving
- CAR Issue and Closing
- Mg't of NCR (From ANR Issue to Closing)
- QA Education and Training

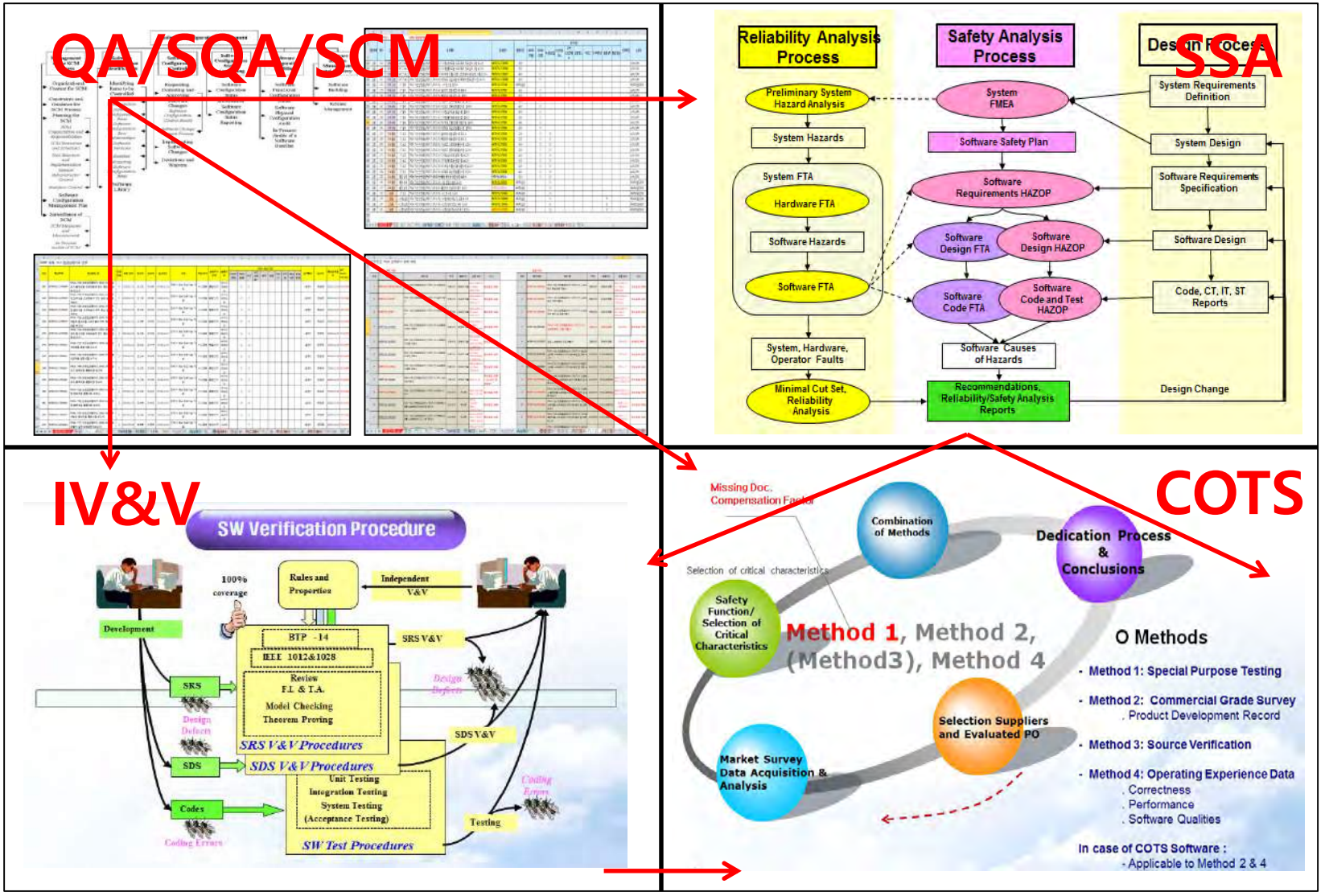
P D C A

- **Safety and Reliability**
- **Licensing Suitability**

Concept of V&V



Relationship of COTS, SSA, IV&V and SCM



Relationship of V&V and other assurance

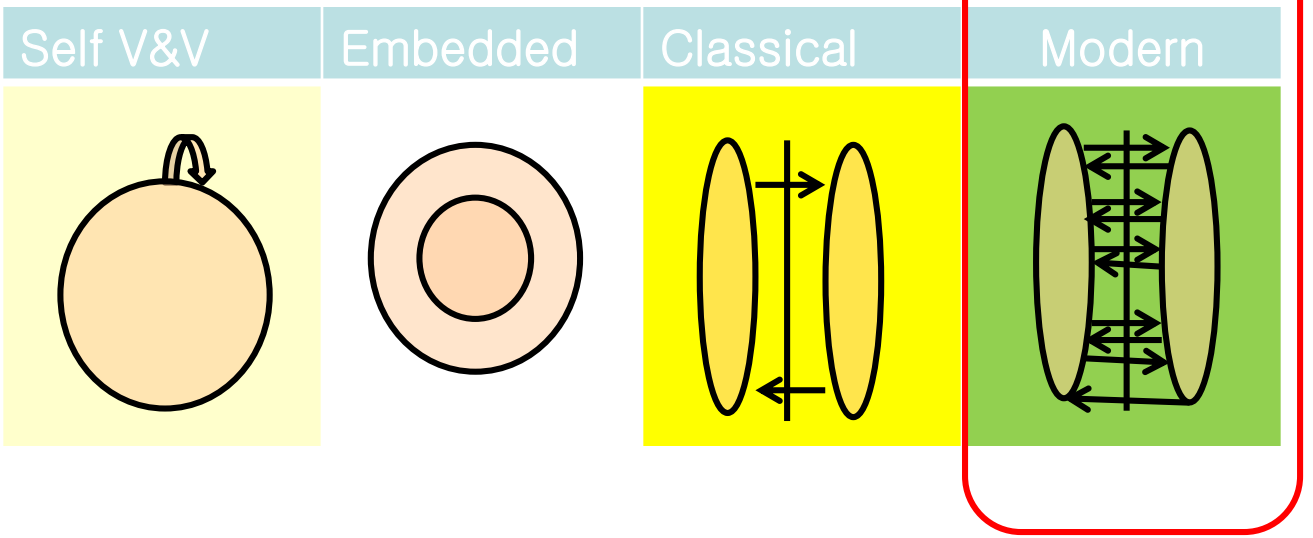
NO	Q	Role and Responsibility(R&R)	
1	SQA	Preparing SQAP Performing of Review Performing of In-process audit	
2	SCM	Preparing SCMP Performing of Functional Configuration Audit and Physical Configuration Audit	
3	SVV	Preparing SVVP Analysis of traceability Testing Supporting of SQA review Supporting of SSA on COTS dedication	QA,Eng, Dev.
4	SSA	Software Safety Analysis based on tracing information on SVV COTS Software Evaluation	

Independence V&V Model

- In the combination of three parameter(Technical, Managerial and Financial) (IEEE Std-1012)
  - Self-V&V
  - Embedded V&V
  - Classical Independent V&V
  - Modern interactive V&V

O Cross Reference Criteria
- IEEE Std. 7-4.3.2
- ASME/NQA-1 2a part 2.7
- IEC Std-987 part 6.2
- IEC Std-60880
- RTCA DO-178B
- UK MODOO-55 Clause 15
- IEEE Std-1012

(No Interaction) (Many interaction)



Classical IV&V :
Modified IV&V : Requirement
Internal iV&V : Requirement
Embedded V&V :

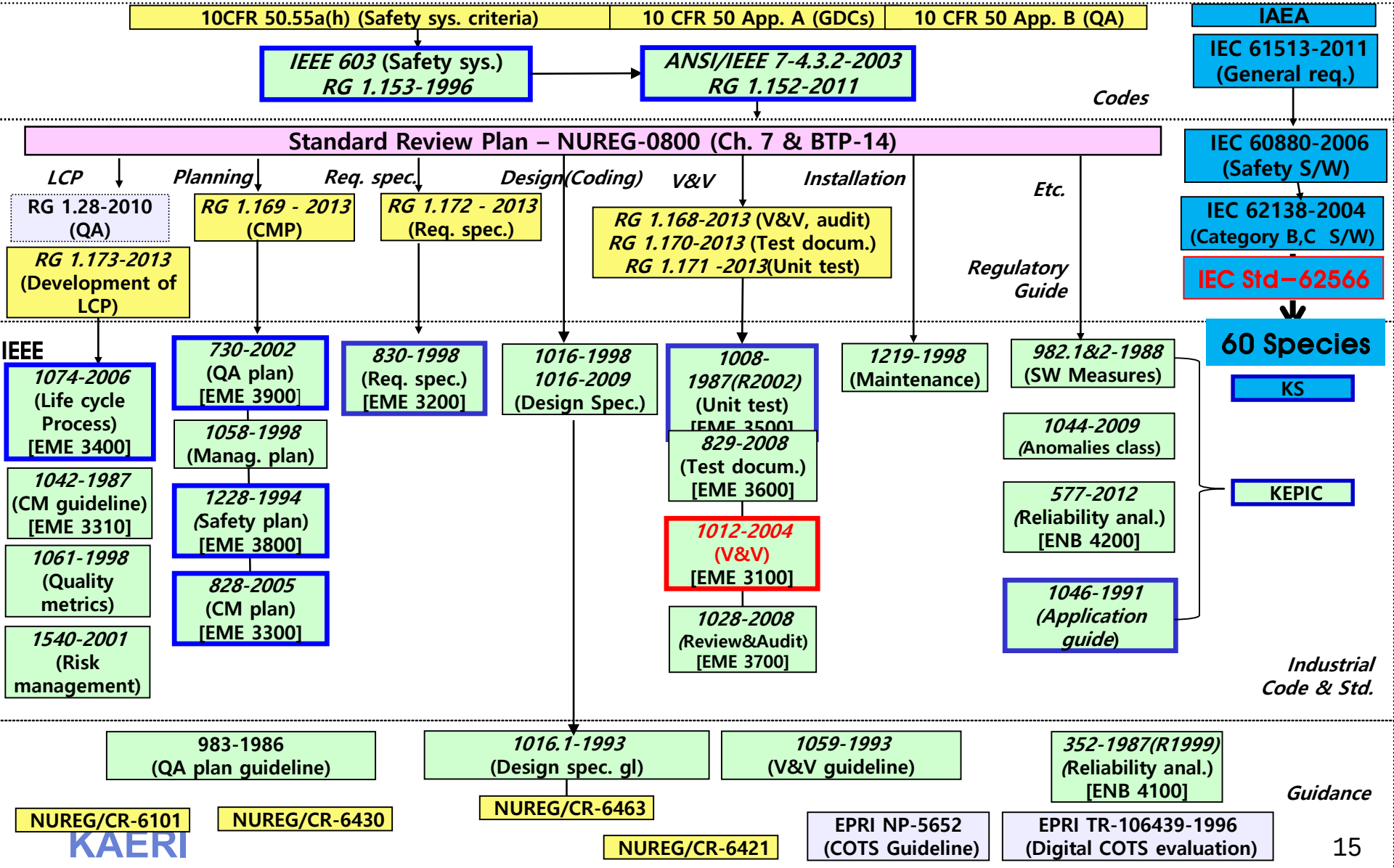
Criteria for Traceability

- NPP Sys. Level : SR, IR and DS
- Forward <-> Backward
  - FPGA/SW : DS

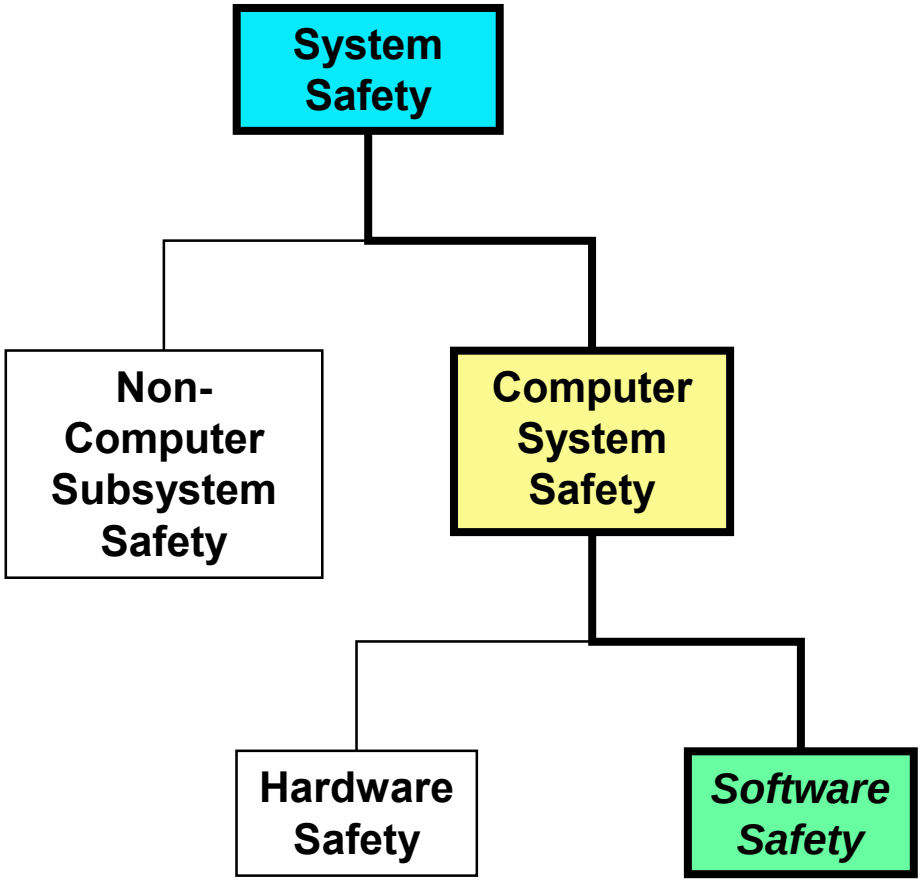
Req. ID	DS		SRS		Review Comments
	TOC/Sec	Description	TOC/Sec	SRS Req.	

Design Phase : Anomaly Report(ANR)
Test Phase : Test Exception Report(TER)

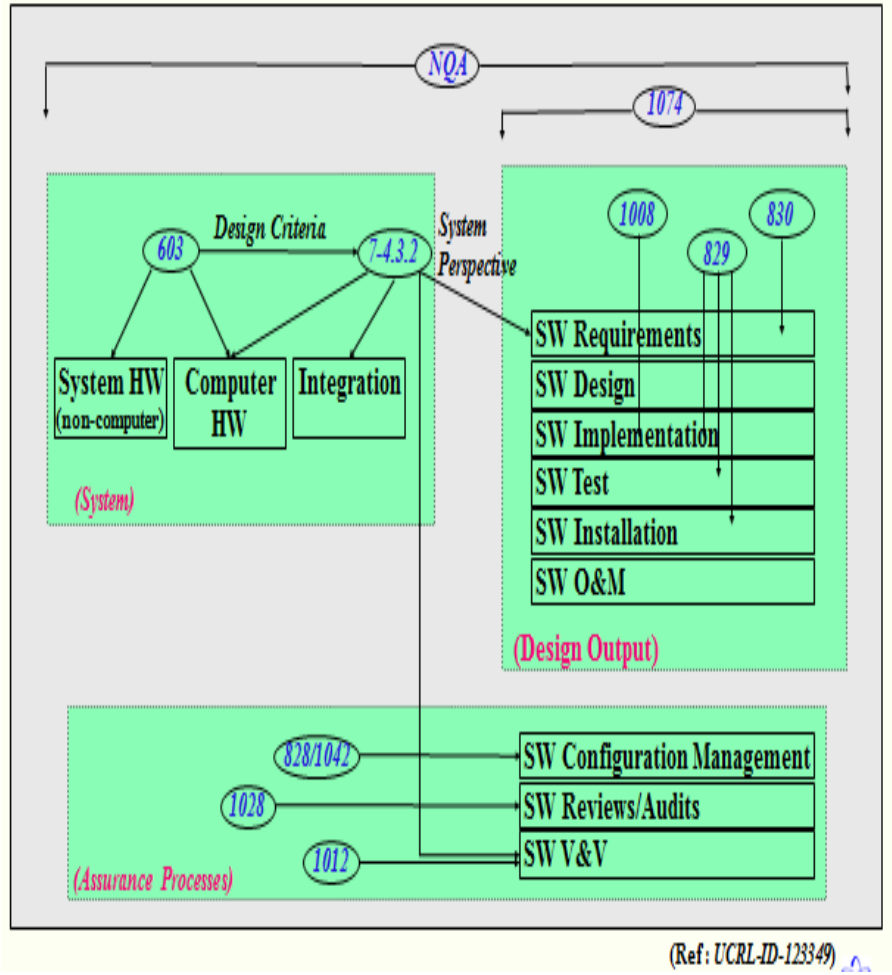
Licensing Requirement



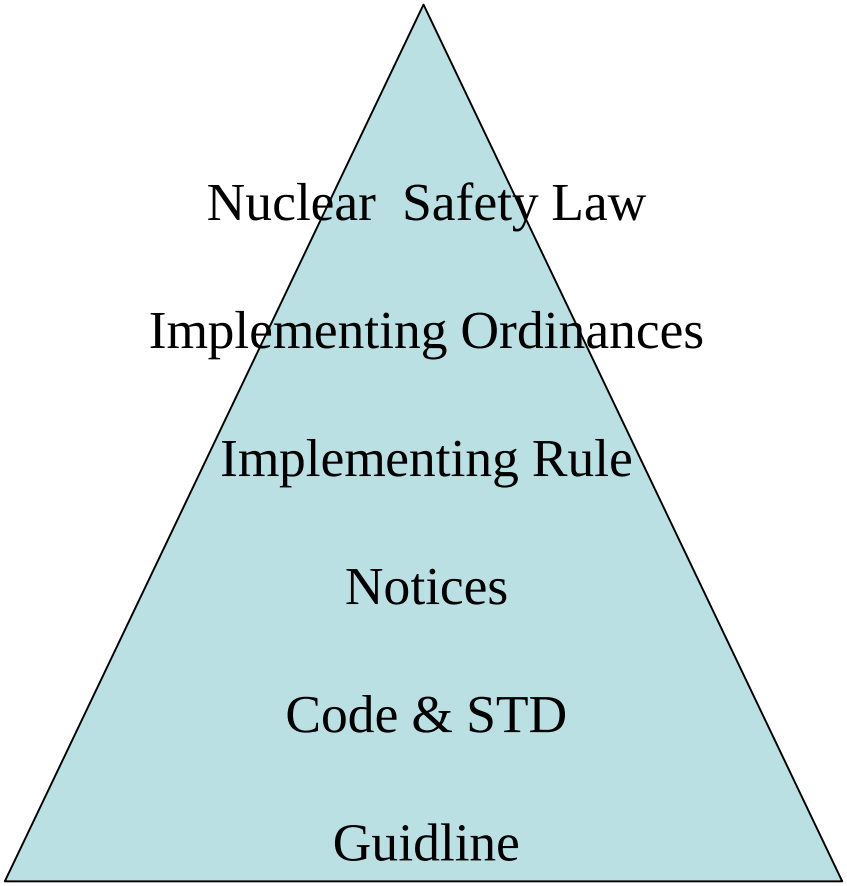
V&V Requirement : Where am I?



(BTP-14)



Compliance Code & STD



IEEE Std 7-4.3.2	Digital Computer Safety
IEEE 1012, IEEE 1028	SW V&V, Review&Audit
IEEE 828	SCM
IEEE 829	SW Test Doc.
IEEE 1008	Unit Test
IEEE 830	SRS
IEEE 1074	SWLC
EPRI-TR-106439	Qualification for COTS
BTP-14	SW Review Gud.
EPRI-TR-107330	PLC Eval Gud.

IEC Std-62566 [+]

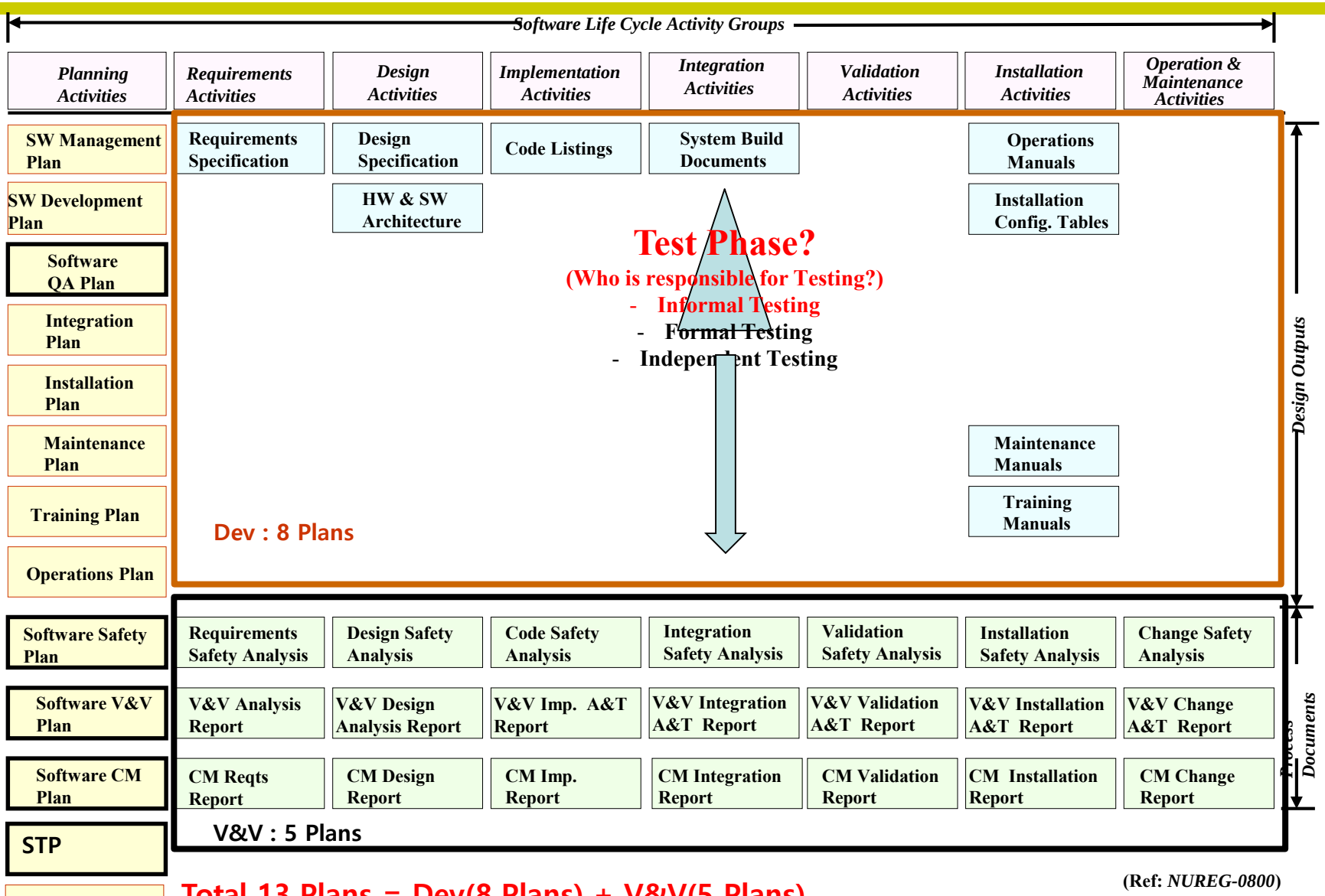
Other Related Standards

Important to Safety System

Safety System (Class1E)

	IEC60987 Computer based Hardware	
RG1.152/IEEE7-4.3.2 Safety grade Digital Computer	IEC61500 Cat A Data Communication	
RG1.173/IEEE1074 SWLC Process	IEC60880 Cat A Functional Software	IEC62138 Cat B/ Cat C Functional Software
RG1.168/IEEE1012,1028 Software V&V, Review & Audit		
RG1.169/IEEE828 Software Configuration Management		
RG1.171/IEEE1008 Software Unit Test		
RG1.170/IEEE Std-829 Software Test Documentation		
RG1.172/IEEE Std-830 Software Requirement Specification		
	IEC62566 HDL Implementation Equipment Usage	
	IEC62645 Computer based System Security	
	IEC62671 Industrial Digital Equipment Usage	

NUREG-0800/BTP-14



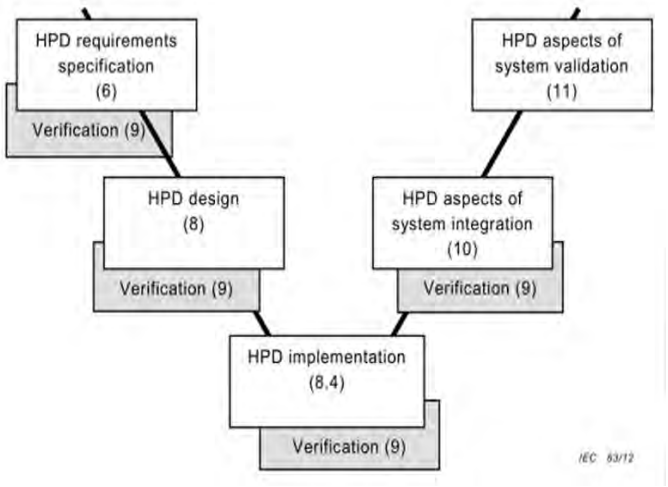
Total 13 Plans = Dev(8 Plans) + V&V(5 Plans)

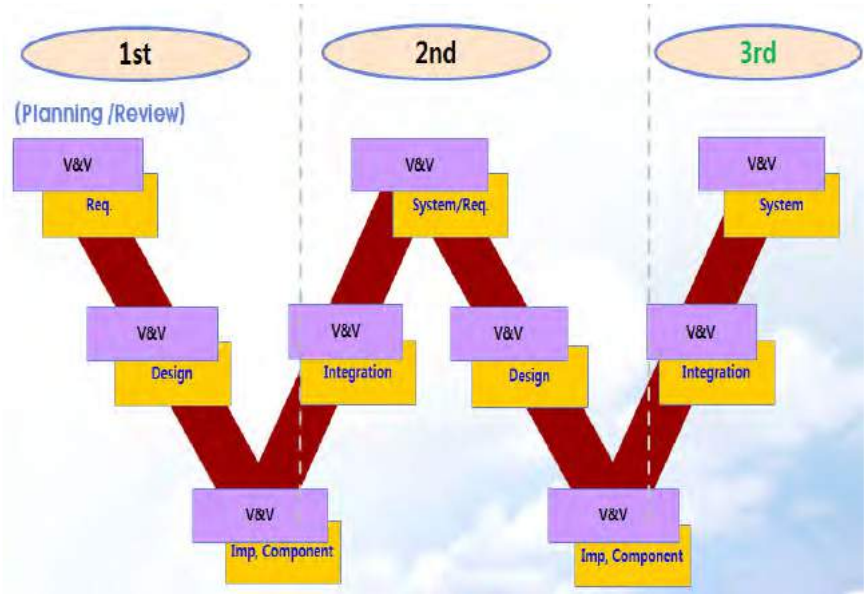
(Ref: *NUREG-0800*)

SWLC : V+V=W Model

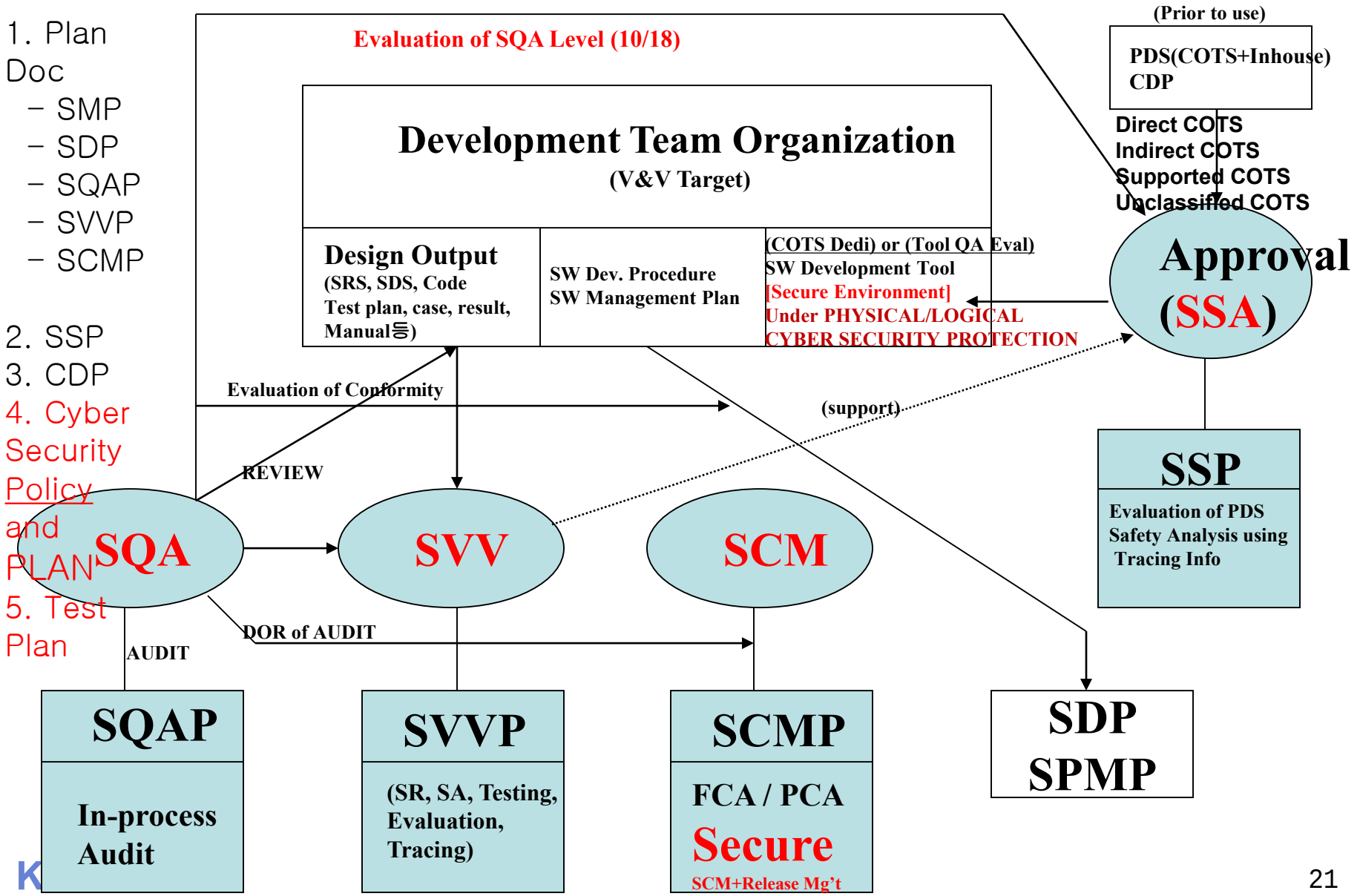
V+V=W

- After 1st V and 2nd V
  - Simple
  - Combined (Modified or Mixed)
  - Full





NUREG 0800/BTP-14 : Software Qualification



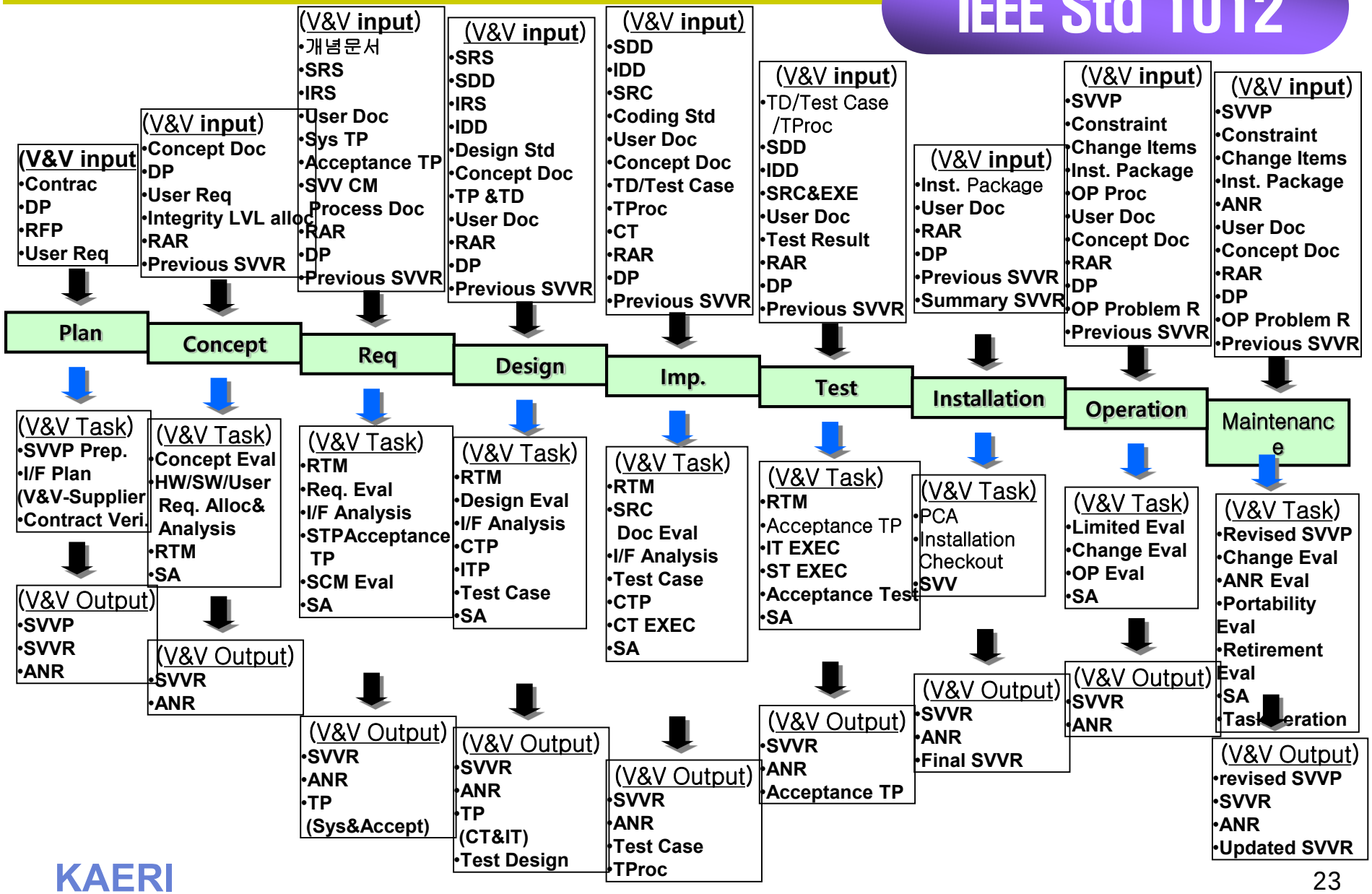
Mapping of Acceptance Framework

- Document Distribution Approval(DDA)
  - Peer Review & Comments
  - Prepared By-**IR By**-Reviewed By-Approved By

- Packing Policy : 13 Planning Doc.
  - DOR(Dev) : SMP, SDP, SIntP, SinstP, SmaintP, STrnP, SOP, SDOEP
  - DOR(V&V) : SQAP, SCMP, SSP, SVVP, STP,
    - Additional Two Plans(STP & SDOEP) : BTP HICB-14, 2007, Rev. 5

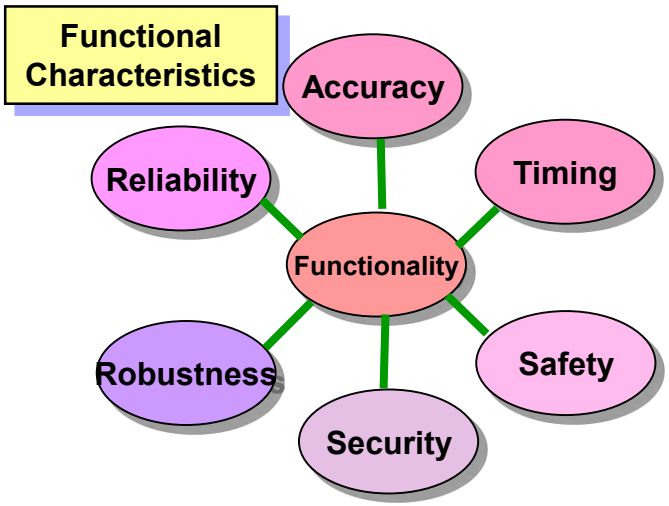
[1012] V&V input–Tasks–V&V Output

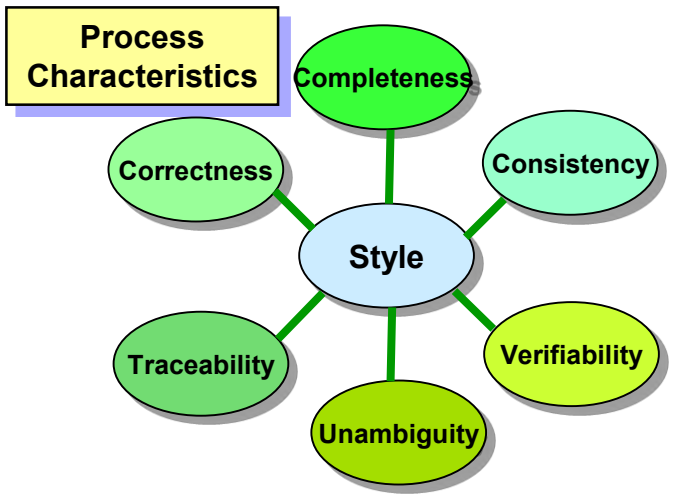
IEEE Std 1012



BTP–14 : Functional vs Process

	Functional Char.	Process Char.
Quality Attributes	Accuracy, Functionality, Reliability, Robustness, Safety, Security, Timing	Completeness, Consistency, Correctness, Style, Traceability, Unambiguity, Verifiability





IEEE Std-1012

Traceability Analysis	Software Requirements Evaluation	Interface Analysis
Correctness Consistency Completeness Accuracy	Correctness Consistency Completeness Accuracy Readability Testability	Correctness Consistency Completeness Accuracy Testability

BTP-14 vs IEEE Std-1012

Evaluation Reault	No. of Acceptable Quality Attribute	BTP-14 Quality Attribute Criteria
Satisfy	14	Accuracy, Functionality, Reliability, Robustness, Safety, Security, Timing, Completeness, Consistency, Correctness, Style, Traceability, Unambiguity, Verifiability
Needed Modify	0	N/A
Not Satisfy	0	N/A
Not Applicable	0	N/A

Evaluation Reault	No. of Quality Atttribute Acceptable	IEEE Std. 1012 Quality Attribute Criteria
Satisfy	13	TA[1] (Correctness, Consistency, Readability, Accuracy) SRE[2] (Correctness, Consistency, Completeness, Readability, Testability) IA[3] (Correctness, Completeness, Accuracy, Testability)
Needed Modify	0	N/A
Not Satisfy	0	N/A
Not Applicable	2	SRE[2] (Accuracy) IA[3] (Consistency)

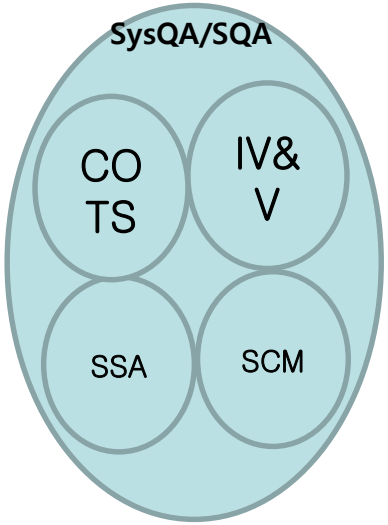
TA[1]: Traceability Analysis
SRE[2]: Software Requirement Evaluation
IA[3]: Interface Analysis

IEC Std-62566 Criteria

Framework	Key Req.	IEC 62566:2012 Criteria	Compliance	Comments
Organization	IV&V	9.1.1~9.1.4	Communication Channel	T, M, F
QA/SQA	QAM/QAP	5.4 HPD quality assurance plan Higher Level Std. : ASME/NQA-1(NUREG-0800/BTP-14)	From Issue to Ending	ANR/TER
COTS	Tool Qualification	9.3 Verification of the use of the Pre-developed Items	Comparison, Dedication	OER
SSA	Safety Analysis			Defense Design
SVV	[Design/Test] HPD, Sys Integration, Sys Validation	[9.1.6, 9.1.7, 9.1.9, 9.1.10] 9.2 Verification Plan, 9.4 Verification of the Design and Implementation, 9.5 Test-benches 9.6 Test Coverage, 9.7 Test Execution, 9.8 Static Verification {9.4, 9.5(9.5.1, 9.5.2), 9.6(9.6.1, 9.6.3, 9.6.4), 9.7(9.7.1, 9.7.2. 9.7.3), 9.8} 10.2.2 System Integration Plan 10.4 Integrated System Verification {10.4.2, 10.4.4, 10.4.7} 10.6 Integrated System Test Report 12.2 System Validation {11.2.1, 11.2.2, 11.2.3, 11.3.1, 11.3.2}	All design output vs V&V	Module-Unit-System Integration
SCM	DOC/Code	5.5 Configuration management	Thread PATH	Level of Depth

Summary of IEEE Std-1012 VS IEC Std-62566

Major/(Supporting)
SysQA(SQA)
SQA(SCM)
SVV(SSA)
SSA(SVV)
COTS(SSA)



SW Concept V&V	→	HPD Concept
SW Req. Analysis V&V	→	HPD Req. Analysis
SW Design V&V	→	HPD Design
Implementation V&V	→	Implementation -Functional Simulation -Logic Simulation -P&L Simulation
Test V&V(CT, IT, ST)	→	HPD System Integration
Installation and Checkout	→	HPD System Validation

* HDL-Programmed Devices(HPD)

IEEE Std-1012 oriented V&V : Embedding IEC Std-62566

SWLC	IEEE Std-1012	IEC Std-62566
Concept	1012	<- (Added) Quality attributes
SRS	1012	<- (Added) Quality attributes
SDS	1012	<- (Added) Quality attributes
Imp.	1012 + NUREG 7006	-
Test	1012	<- IEC Std-62566
Installation and Check out	1012	<- IEC Std-62566

Compiling of Planning phase Criteria

Management Characteristics	Implementation Characteristics	Implementation Characteristics
Purpose	Measurement	Budget
Organization	Procedures	Methods/tools
Oversight	Record keeping	Personnel
Responsibilities	Schedule	Standards
Risks		
Security		

SRS/SDS V&V Pass/Fail Criteria

1. SRS Evaluation
   - Licensing Suitability : BTP-14 (Functional Characteristics, Process Characteristics)
     . Functional Characteristics : Accuracy, Functionality, Reliability, Robustness, Safety, Security, Timing
     . Process Characteristics : Completeness, Consistency, Correctness, Style, Traceability, Unambiguity, Verifiability
   - Detailed Doc. Evaluation : IEEE Std-1012 based
     . Traceability Analysis : Correctness, Consistency, Completeness, Accuracy
     . SW Req. Evaluation : Correctness, Consistency, Completeness, Accuracy, Readability, Testability
     . I/F Analysis : Correctness, Consistency, Completeness, Accuracy, Testability

2. SRS Traceability : Key Requirement
   - Internal : Section by Section
   - External : Upper – Lower

3. Issuing Anomaly report

Evaluation Result	Regulatory Basis and Standards	Action
Satisfy	Fully reflected[1)]	Acceptable
Needed Modify	Properly reflected[2)]	Modification
Not Satisfy	Not reflected[3)]	Revision
	To be determined/Later[4)]	Revision
Not Applicable	Not Applicable[5)]	Acceptable

Compiling of Requirement phase Criteria

Check List for Requirement Phase Software V&V Checklist for BTP-14

Appendix A. Requirement Phase Software V&V Checklist for BTP-14

Classification	Detail Characteristic	ID	Evaluation Item	Evaluation result and Comment (FPM-01)	ANR No
Functional characteristic (B.3.3.1.1)	Accuracy	VR01-01	Accuracy requirements should be provided for each input and each output variable.		
		VR01-02	Accuracy requirements should be stated numerically, and appropriate physical units and error bounds should be supplied.		
		VR01-03	Accuracy requirements should include a description of data type and data size for each input and output variable.		
	Functionality	VR02-01	Functionality requires that the operations that must be performed for each mode of operation be completely specified.		
		VR02-02	Functions should be specified in terms of inputs to the function, transformations to be carried out by the function, and outputs generated by the function.		
	Reliability	VR03-01	Reliability requires that all requirements for fault tolerance and failure modes be fully specified for each operating mode.		
		VR03-02	Software requirements for handling both hardware and		

Appendix B. Requirement Phase Software V&V Checklist for IEEE Std-1012

Appendix B. Requirement Phase Software V&V Checklist for IEEE Std.1012

Classification	Detail Characteristic	ID	Evaluation Item	Evaluation result and Comment (FPM-01)	ANR No
Traceability Analysis (Table 1c 9.2)	Correctness	VR15-01	Are the relationships between each software requirement and its system requirement correct?		
	Consistency	VR16-01	Are the relationships between the software and system requirements specified to a consistent level of detail?		
	Completeness	VR17-01	Is every software requirement traceable to a system requirement with sufficient detail to show conformance to the system requirement?		
		VR17-02	Are all system requirements related to software traceable to software requirements?		
	Accuracy	VR18-01	Are the system performance and operating characteristics accurately specified by the traced software requirements?		
Software Requirements Evaluation (Table 1c 9.2)	Correctness	VR19-01	Do the software requirements satisfy the system requirements allocated to software within the assumptions, constraints, and operating environment for the system?		
		VR19-02	Do the software requirements comply with standards, references, regulations, policies, physical laws, and business rules?		

Needed insert column : Status(Open/Close, N/A etc.) after Rev. 0

Compiling of Design phase Criteria

Check List for SAD & SDS Phase Software V&V Checklist for BTP-14

Appendix B. Design Phase Software V&V Checklist for IEEE Std-1012

A-1. Design Phase Evaluation for Software Architecture Description (SAD) in Design Activities

Classification	Detail Characteristic	ID	Evaluation Item	Evaluation result and Comment (FPM-01)	ANR No
Functional Characteristic (B.3.3.2.1)	Reliability	VD01-01	Reliability requires that the combined hardware and software architecture be such that individual software element failure will not compromise safety.		
		VD01-02	The software architecture should identify actions to be taken in the event of error detection.		
		VD01-03	The hardware and software architecture should be reviewed to verify that the propagation of errors is controlled via a well-structured modular design.		
	Safety	VD02-01	Safety requires that the software architecture introduce no new hazards into the safety system.		
		VD02-02	The safety functions should be separated from normal operating and overhead functions, with well-defined and strictly controlled interfaces between them.		

A-2. Design Phase Evaluation for Software Design Specification (SDS) in Design Activities

Classification	Detail Characteristic	ID	Evaluation Item	Evaluation result and Comment (FPM-01)	ANR No
Functional Characteristic (B.3.3.3.1)	Accuracy	VD10-01	Accuracy requires that all calculations be specified in such a way that the accuracy requirements for the calculations will be satisfied.		
		VD10-02	Floating point arithmetic should be avoided; if that is not possible, special care must be taken to maintain the accuracy of the calculations.		
		VD10-03			

Appendix B. Design Phase Software V&V Checklist for IEEE Std.1012

Classification	Detail Characteristic	ID	Evaluation Item	Evaluation result and Comment (FPM-01)	Note
Traceability Analysis (Table 1c 9.3)	Correctness	VD22-01	Is the relationship between each design element and the software requirement(s) correct?		
	Consistency	VD22-02	Are the relationships between the design elements and the software requirements specified to a consistent level of detail?		
	Completeness	VD22-03	Are all design elements traceable from the software requirements?		
		VD22-04	Are all software requirements traceable to the design elements?		
Software Design Evaluation (Table 1c 9.3)	Correctness	VD25-01	Does the software design satisfy the software requirements?		
		VD25-02	Does the software design comply with standards, references, regulations, policies, physical laws, and business rules?		
		VD25-03	Did the design sequences of states and state changes using logic and data flows couple with domain expertise, prototyping results, engineering principles, or other basis?		

Compiling of Implementation phase Criteria

- Implementation Phase Software V&V Checklist for BTP-14
- Implementation Phase Software V&V Checklist for IEEE Std-1012
- NUREG/CR-7006 Code Review Checklist

▪ Appendix A. Implementation Phase Software V&V Checklist for BTP-14

Classification	Detail Characteristic	ID	Evaluation Item	Evaluation result and Comment (FPM-01)	ANR No.
Functional Characteristic	Accuracy	VIP01-01	Accuracy requires that the actual source code be written so that the accuracy requirements and accuracy design specifications are met.		
		VIP01-02	Special care should be taken for floating point arithmetic, round-off errors, and the retention of precision during numerical operations.		
		VIP01-03	If mathematical subroutine libraries are used, the accuracy characteristics of the subroutines should be known and documented, and shown to meet the accuracy requirements and accuracy design specifications.		
	Robustness	VIP02-01	Robustness requires that the system be coded in such a way that corrupted data will not cause the safety system to fail.		

▪ Appendix B. Implementation Phase Software V&V Checklist for IEEE Std. 1012

Classification	Detail Characteristic	ID	Evaluation Item	Evaluation result and Comment (FPM-01)	ANR No.
Traceability Analysis	Correctness	VIP12-01	Are the relationships between source code components and design elements correct?		
	Consistency	VIP13-01	Are the relationships between the source code components and design elements specified to a consistent level of detail?		
	Completeness	VIP14-01	Is every source code components traceable from the design elements?		
		VIP14-02	Are all design elements traceable to the source code components?		

▪ Appendix C. Implementation Phase Traceability Matrix

Traceability analysis for SDS, Code List, and Code							
SDS		Code List		Code			Note
Section	Sub Section	File name	Lower File name	File Name	Module name	Lower File name	
CLFPM01 Control Logic I/F Signal	CLFPM01_APP_INTERFACE	clfpm01_top	clfpm01_app_intf	clfpm01_top	CLFPM01_APP_INTERFACE	clfpm01_app_intf	
	CLFPM01_DATALINK_HANDLER		clfpm01_datalink_handle		CLFPM01_DATALINK_HANDLER	clfpm01_datalink_handle	
	CLFPM01_CHECK_NORM_P33GD		clfpm01_diag_proc_p33v				
	CLFPM01_DISPLAY_STATUS		clfpm01_display_led		CLFPM01_DISPLAY_STATUS	clfpm01_display_led	
	CLFPM01_GEN_RESET_CLOCK		clfpm01_gen_reset_clk		CLFPM01_GEN_RESET_CLOCK	clfpm01_gen_reset_clk	
	CLFPM01_IO_MODULE_HANDLER		clfpm01_iom_sbus_handle		CLFPM01_IO_MODULE_HANDLER	clfpm01_iom_sbus_handle	
	CLFPM01_INTERNAL_MEMORY		clfpm01_mem		CLFPM01_INTERNAL_MEMORY	clfpm01_mem	
	CLFPM01_NVSRAM_BI_DIR_DATA_SEL		clfpm01_nvm_bi_dir_data		CLFPM01_NVSRAM_BI_DIR_DATA_SEL	clfpm01_nvm_bi_dir_data	
	CLFPM01_NVSRAM_HANDLER		clfpm01_nvm_handle		CLFPM01_NVSRAM_HANDLER	clfpm01_nvm_handle	
	CLFPM01_NETWORK_MODULE_HANDLER		clfpm01_nvm_sbus_handle		CLFPM01_NETWORK_MODULE_HANDLER	clfpm01_nvm_sbus_handle	
	CLFPM01_INDICATION_PATTERN		clfpm01_pattern_tx_sig		CLFPM01_INDICATION_TX_PATTERN	clfpm01_pattern_tx_sig	
	CLFPM01_GEN_CLR_ERRST		clfpm01_psbt_clear		CLFPM01_GEN_CLR_ERRST	clfpm01_psbt_clear	
	CLFPM01_USER_SET_PARAMETER		clfpm01_us_set_param		CLFPM01_USER_SET_PARAMETER	clfpm01_us_set_param	
					CLFPM01_INDICATION_WRITE_NVSRAM	clfpm01_ind_wr_nvm	

▪ Appendix D. NUREG/CR-7006 Code Review Checklist for CLFPM01

Quality Characteristics	Detail Characteristic	ID	Review Item	Significance	Evaluation result and Comment (FPM-01)	Note
2.1 Reliability	2.1.2 FPGA Internal Logic Design Attributes	Asynchronous Design	CR01-01 The FPGA design should be synchronous as much as possible. Asynchronous designs are prone to glitches, bus skews, and other timing issues. Furthermore, the FPGA design tools do not generally support asynchronous timing constraint and analysis.			
			CR01-02 If asynchronous designs are used for 100% testability or any other reason, appropriate measures need to be taken to make sure that the output glitches and the bus skews are not affecting safe operation of the FPGA design.			
			CR01-03 These measures may include use of registered I/Os or analog filtering of the FPGA outputs.			
		Metastability	CR02-01 Metastability can occur when an asynchronous input gets clocked within the FPGA, and it is expressed as an undetermined state at the output of a flip-flop.			
			CR02-02 The undetermined state resolves itself after the recovery time, which is on the order of several ns to several tens of ns for most of FPGAs.			

Compiling of Test phase Criteria

- Component Test : Statement, Branch/Condition
- Integration Test : Load Balance, Resource(Memory Leak…)
- System Test : Functional, Performance, Interface, Error Injection

Example of V&V task entry and exit criteria

. EX : Component Test

-> Entry Criteria

. Component Test Plan, Test Case Data, Driver(or Stub etc.), Test Platform/Tools

-> Exit Criteria

. Successful of all test coverage

. Statement/Branch/Condition, Expression, Finite State Machine, Line Coverage etc.

Compiling of Installation and Checkout phase Criteria

o Installation &

- Installation configuration Table

. Integration Level –> Phase(Intermediate Combination) -> Target

. Priority & Risk Level

o INPUT – Integration Test Proc. - OUTPUT

(Operation and Maintenance) : Start-up, Operation, and Shutdown, {Updating Procedure}

- Factory Acceptance Test (FAT)
- Site Acceptance Test (SAT)

Conclusion

- How to make a Acceptable Framework?
  - USNRC based IEEE-Std
  - IAEA based IEC-Std
- The Policy of Packing and Flexibility
- Stepping Stone Evaluation on Licensing Suitability
  - Compiling from Acceptable Framework
  - Baseline of Code Cut-off Date

Thank you for your attention