Verification and Validation of FPGA Based Logic Controller

Dec. 6th , 2017

Jang Yeol Kim

KAERI 한국원자력연구원
Korea Atomic Energy Research Institute

– Table of Contents –

- Overview
  - Background：Initiative
- QA/SCM
- SA/COTS
- V&V of SRS, SDS and Imp
- Independent Testing(CT, IT and ST)
- Lic. Compliance Check
- Conclusion

Background

O Needed for 100% Coverage Test for Safety-critical Software

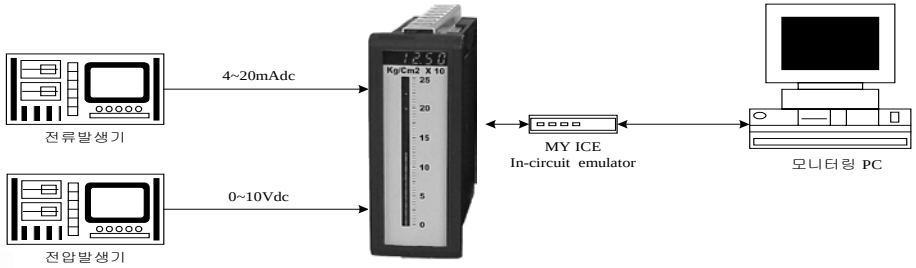
O Manual Test

- Not Cost Effective

- Too much longer time

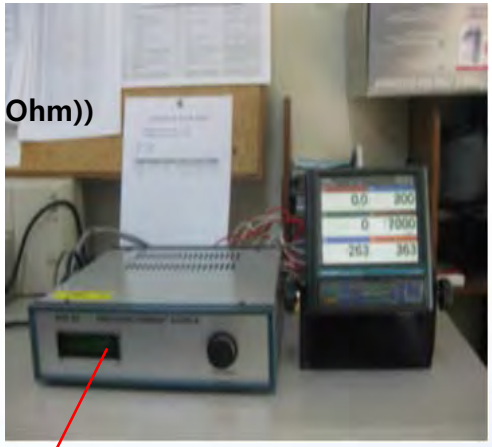
O Needed Exhaustive Testing : Full PATH Testing if possible

Test Experience : Small Digital Devices

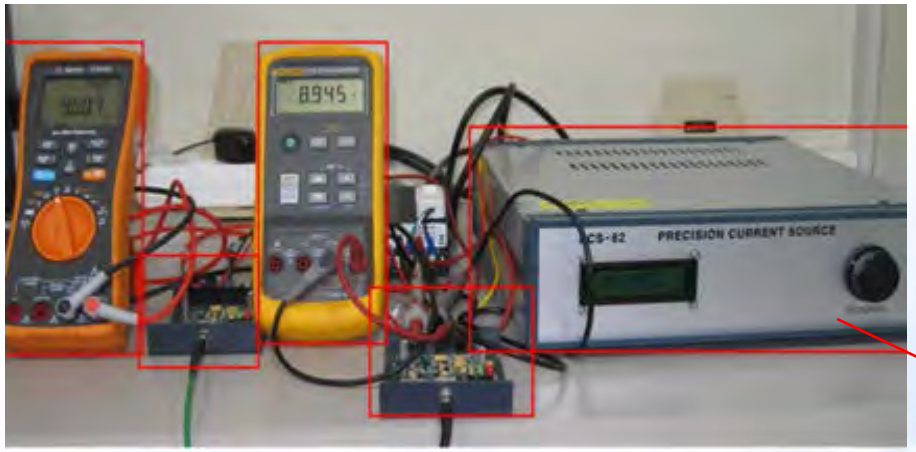


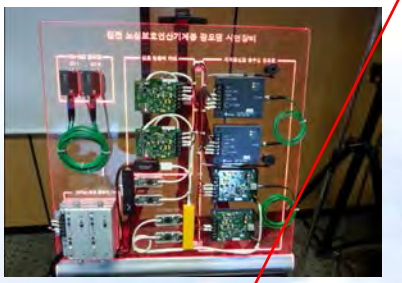
- STEP(2~64) vs DT(01~99)
  - 2ms/STEP
- PUSH/Rotation
- Max/Min

[Voltage : 0.1ms]
[Current : 1.0000V~5.ooV (250 Ohm))



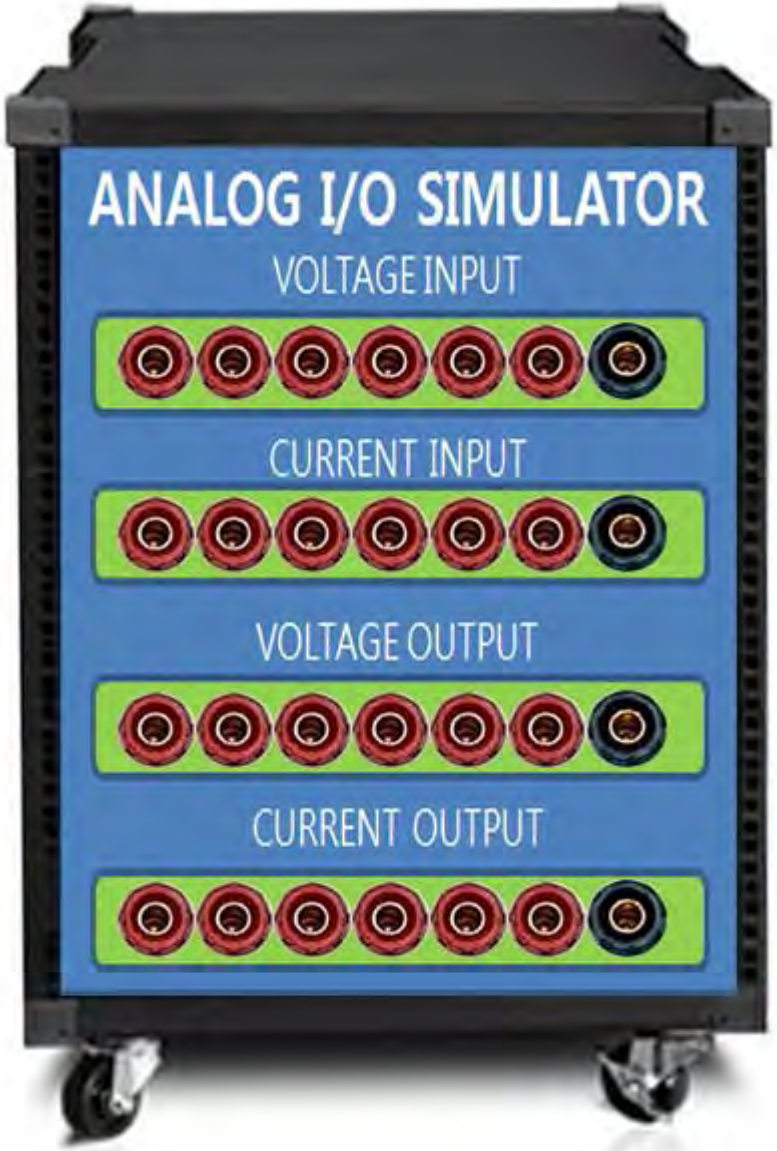
Current : 6CH, Voltage : 2CH

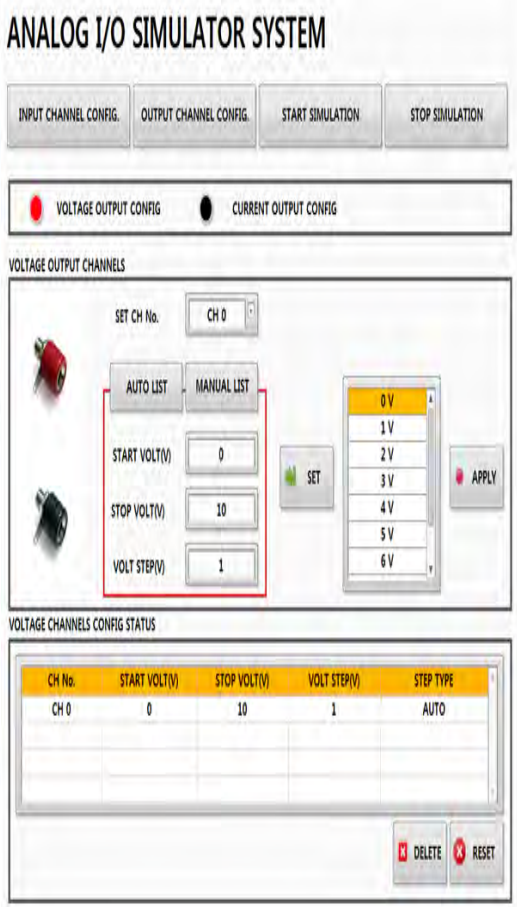




(Automatic Signal Generator)

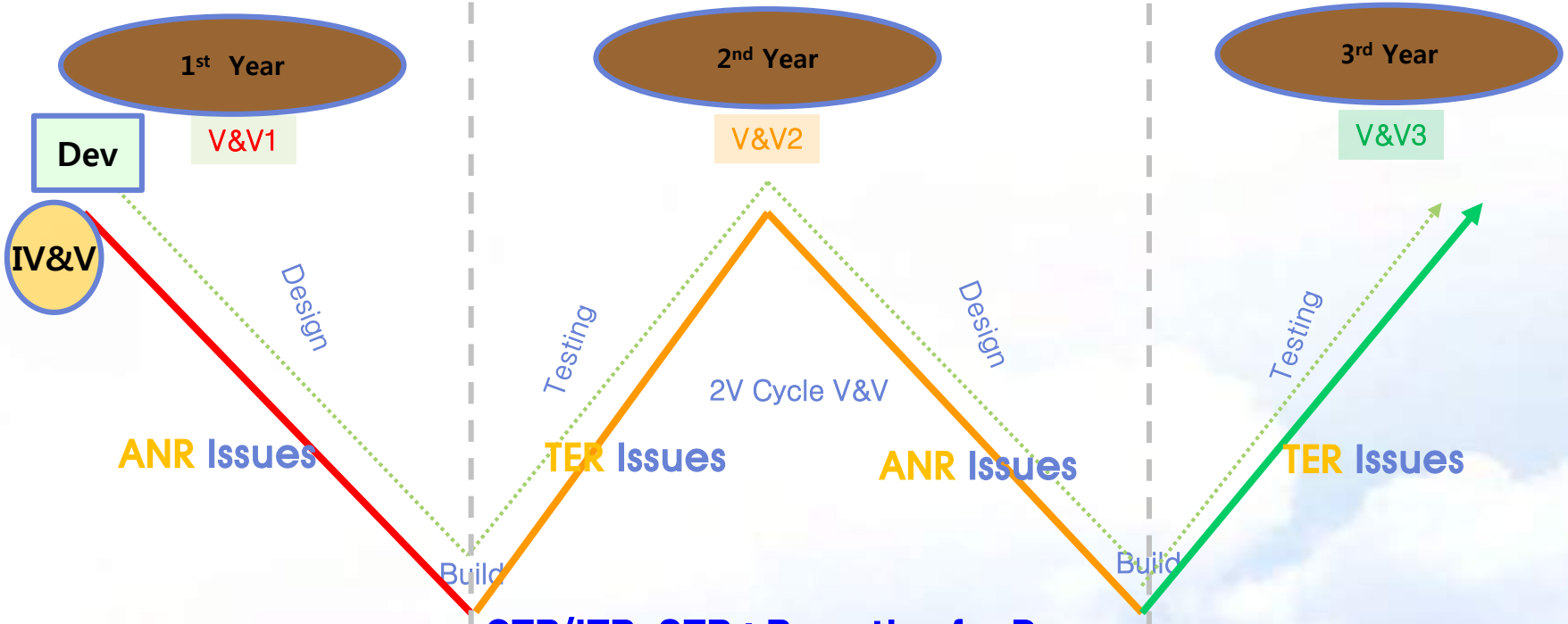
Manufacturing for Stimulator





V&V Schedule (V+V=W Model)

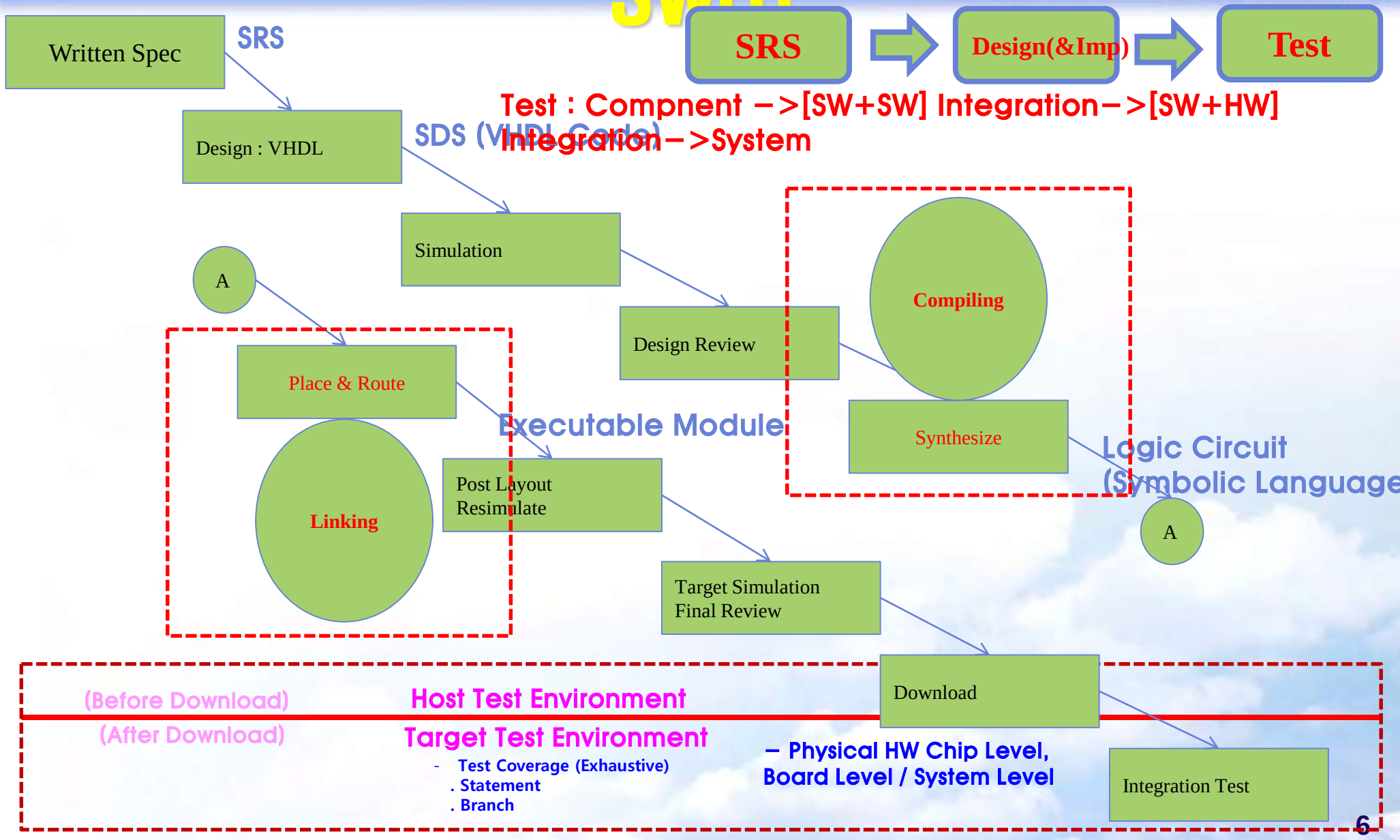
- **Design : ANR, Testing : TER**
- **V-Model Iteration and Re-Verification**



CTR/ITR, STR : Reporting for Dev. Prj :Anomaly Report(ANR), Test Exception Report (TER)
(Test Case Generation/SW-SW, SW-HW, System, Target . Error Injection, Load Balancing / Burning Test ->
Confirmation of Independent Verifier

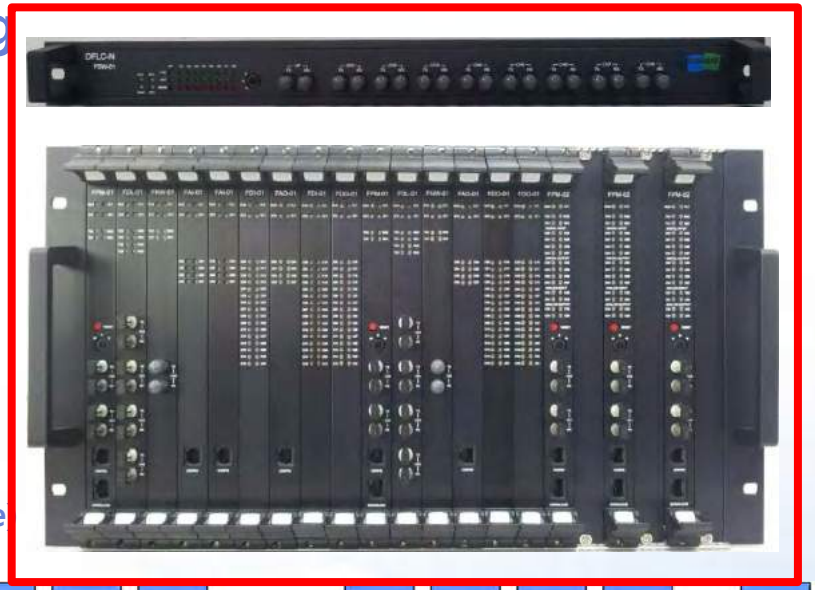
Completion of FLC V&V

What is Difference about Traditional SW LC

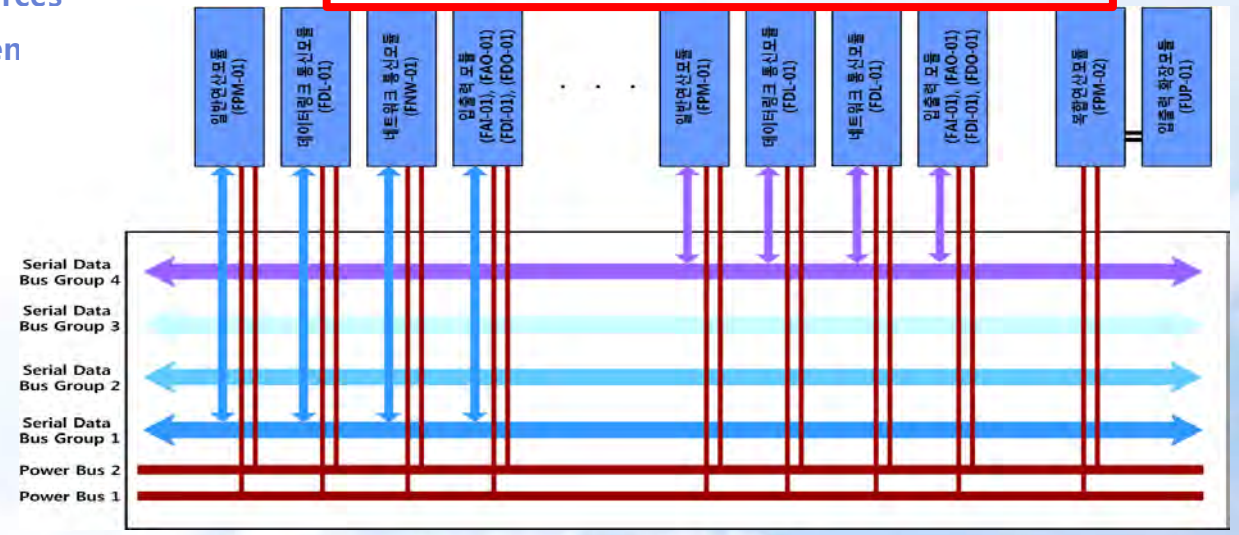


V&V Target : FPGA-based Controller

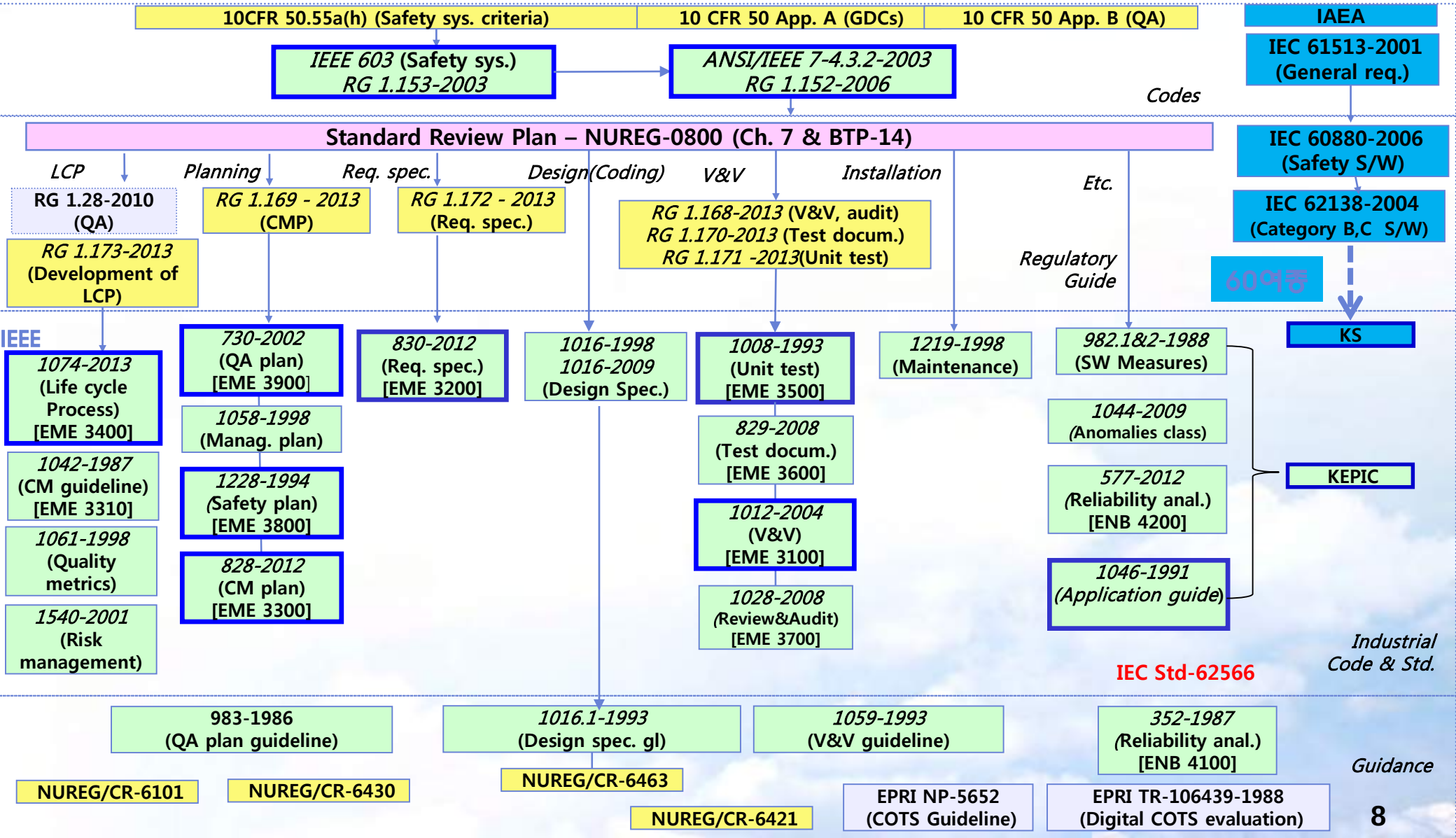
- **Independent Multi-operation Processing**
  - **Maximum : quadruple operation can be processed.**
    - ➢ Four groups of serial bus applied



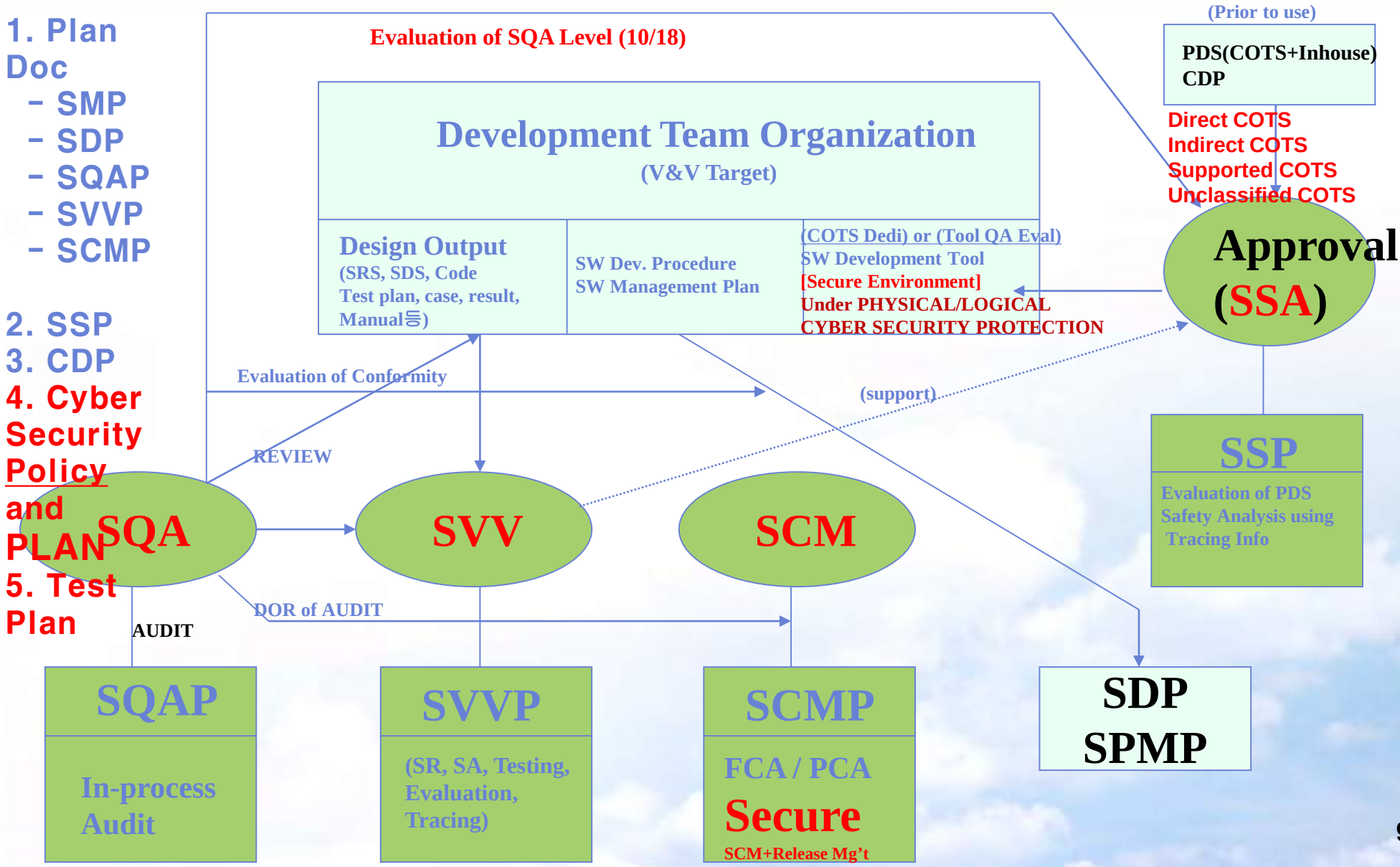
- **Sub Rack**
  - **Size : 19Inch 6U, 21 slot**
  - **Fan less heat dissipation structure (natural air-cooled type)**
  - **Two independent external power sources**
  - **Front : Front Insertion/Removal System**
  - **Rear : I/O terminal Connector**



Licensing Requirement



NUREG 0800/BTP-14 : Software Qualification



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 against CCF**
- **Licensing Suitability**

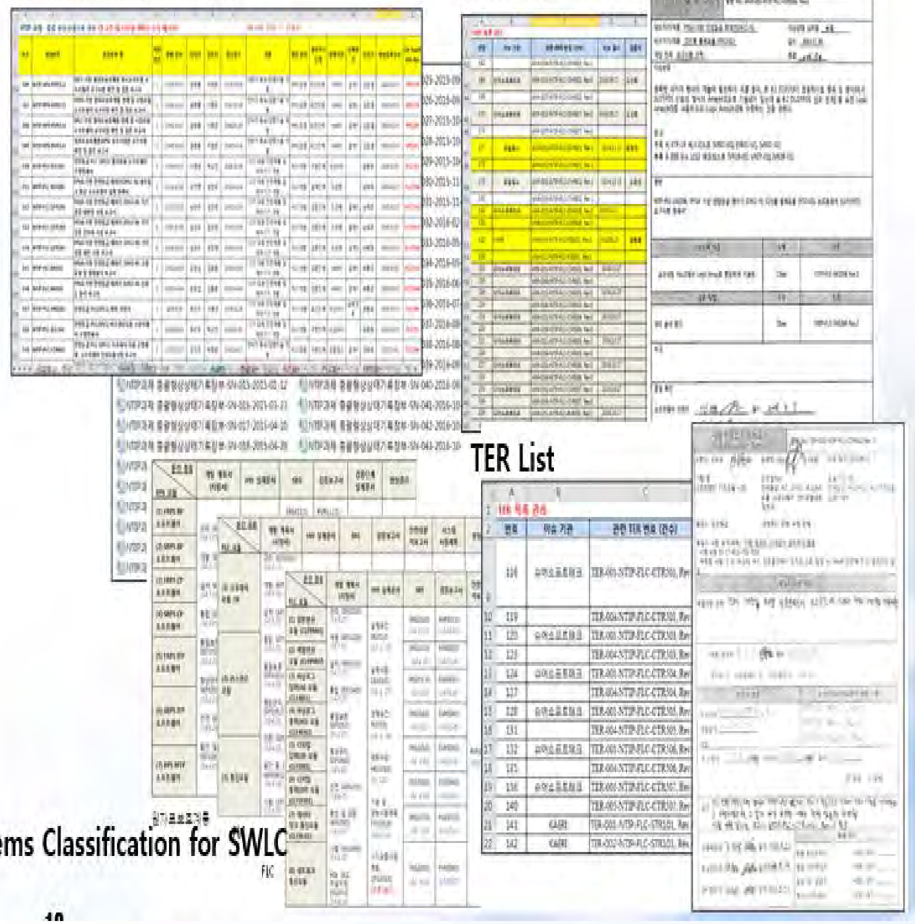
From ANR/TER issues Opening to Closing

Overall Status Record

ANR List

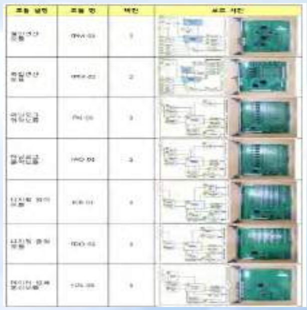
TER List

Items Classification for SWLC



Distribution List

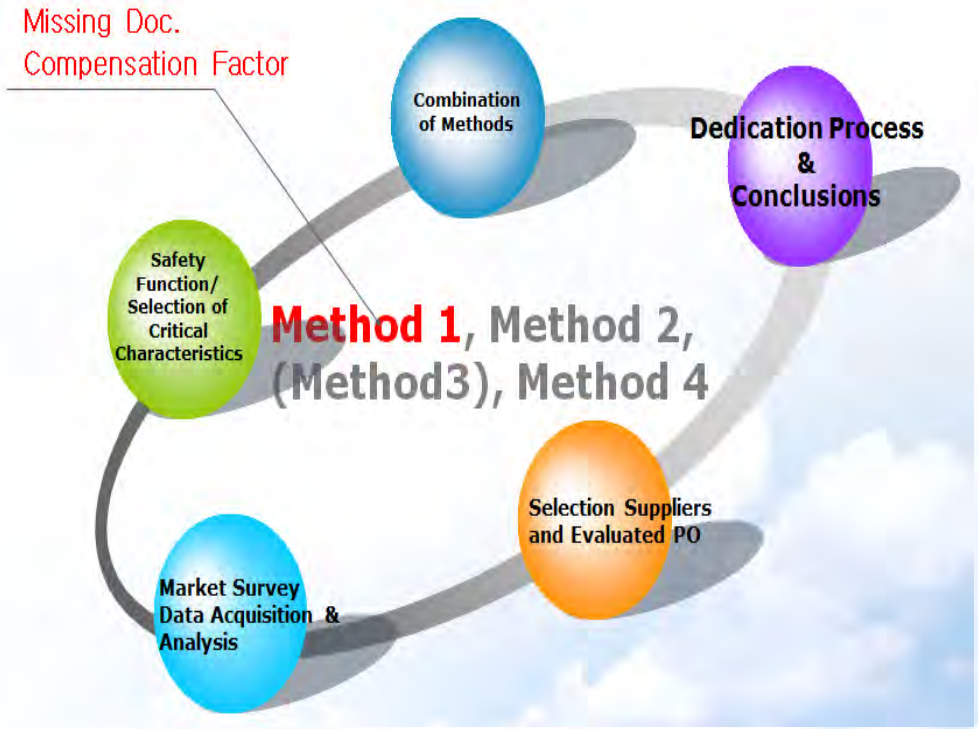
The example of baseline list



Quality Evaluation of COTS SW

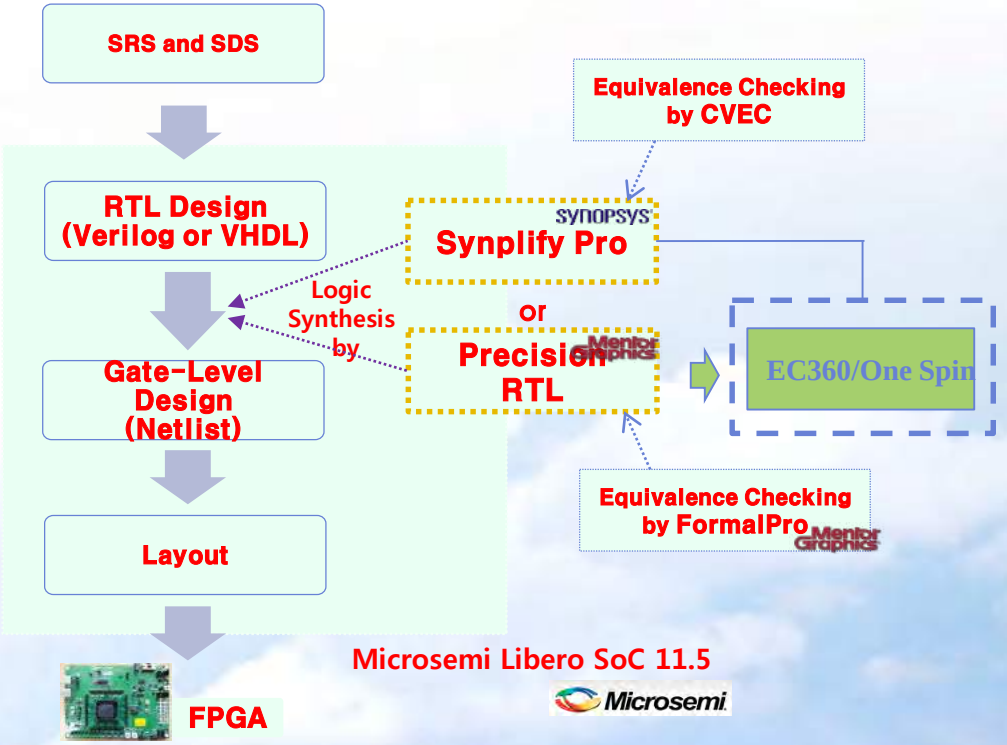
COTS SW Dedication 대상 (by NP-5652/TR-106439 + KINS/RG-17.12)

- Direct SW
- Indirect SW : Ex) Compiler, Environment Toolset
  - NUREG/CR-6421 : Too Strict
  - EPRI-NP-5652 : HW
  - EPRI-TR-106439 : HW+SW



O Methods
- Special Purpose Testing : Method 1
- Commercial Grade Survey : Method 2
  . Product Development Record
- Source Verification : Method 3
- Operating Experience Data : Method 4
  . Correctness
  . Performance
  . Software Qualities

In case of COTS Software : Applicable to Method 2 & Method 4



Safety Analysis of FLC

- **Approaching**
  - **Safety Analysis Plan**
  - **Safety Analysis Guideline**
  - **Deviation : DFLC-N Characteristics**
  - **Experiences from Past Projects**
  - **Tracking of V&V Test Results**
  - **Follow-Up**

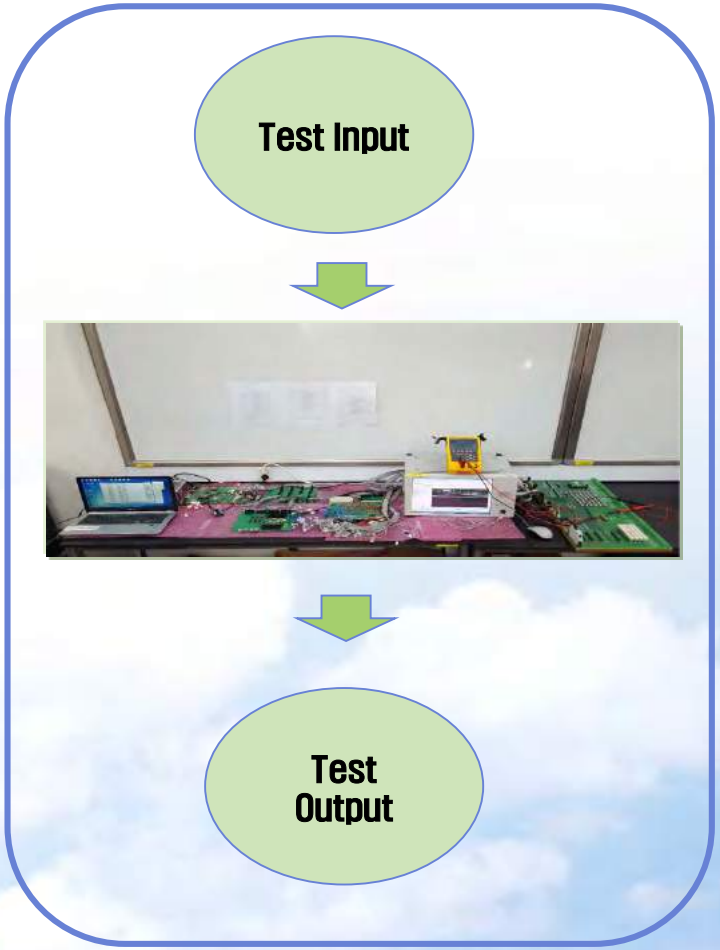
Deviation
HW Initialization Fail
Memory Initialization Fail
Parameter Setup Missing
Initialization Fail for I/O Updating
Malfunction of FPGA
Stuck at all zeros of ROM/RAM
Memory partition assignment fail
WDT Error

Deviation
Execution Error for Functional Spec
Fail for Reset and Clock Generation Function
Violation of Trigger Condition for Reset and Clock Generation
Termination Violation of Reset and Clock Generation
Fail for Operating Voltage Monitoring
Violation of Trigger Condition for Operating Voltage Monitoring
Termination Violation of for Operating Voltage Monitoring
Fail of Memory Setup and Diagnostics
Violation of Trigger Condition for Memory Setup and Diagnostics
Termination Violation of Memory Setup and Diagnostics
Fail of Inter-Module Data Interface
Violation of Trigger Condition for Inter-Module Data Interface
Termination Violation of for Inter-Module Data Interface
Fail of Data Diagnostics
Violation of Trigger Condition for Data Diagnostics
Violation of Termination Condition for Data Diagnostics

Safety Analysis of FLC

Safety Analysis and Safety Test based on Recommended Deviation

Deviation	Recommendatiopn
Execution Error for Functional Spec	Confirmation with V&V of Testing Phase
Fail for Operating Voltage Monitoring	"
Violation of Trigger Condition for Operating Voltage Monitoring	"
Termination Violation of for Operating Voltage Monitoring	"
Fail of Memory Setup and Diagnostics	"
Violation of Trigger Condition for Memory Setup and Diagnostics	"
Termination Violation of Memory Setup and Diagnostics	"
Fail of Inter-Module Data Interface	"
Violation of Trigger Condition for Inter-Module Data Interface	"
Violation of Trigger Condition for Inter-Module Data Interface	"
Fail of Data Diagnostics	"
Violation of Trigger Condition for Data Diagnostics	"
Violation of Termination Condition for Data Diagnostics	"



SRS/SDS V&V Report[1]

1. V&V Method and Criteria

- V&V Activities for SRS
  - IEEE Std 1012 + IEC 62566
  - NUREG 0800 Chapter 7/BTP-14
    - Functional and Process Characteristics

Relationship of IEC 62566 and IEEE 1012

IEC 62566	Phase	IEEE Std 1012-2004	Comments
6.6.1	SRS	- Traceability - SRS Evaluation : Correctness, Completeness, Accuracy, Testability - Interface Analysis : Correctness, Consistency	
6.6.2		- Traceability - SRS Evaluation - Interface Analysis	
6.6.3		- SRS Evaluation : Consistency, Completeness, - Interface Analysis : Consistency, Completeness	
6.6.4		- IEEE Std 1012 Appendix C **V&V Independence**	Technical, Manageable
9.4.1 a)	SDS	- Traceability - Design Evaluation : Completeness, Consistency - Interface Analysis : Completeness, Consistency	
9.4.1 b)		- Design Evaluation : Readability, Testability - Interface Analysis : Testability	
9.4.1 c)		- Traceability - Design Evaluation : Correctness, Consistency, Completeness - Interface Analysis : Correctness, Consistency, Completeness	

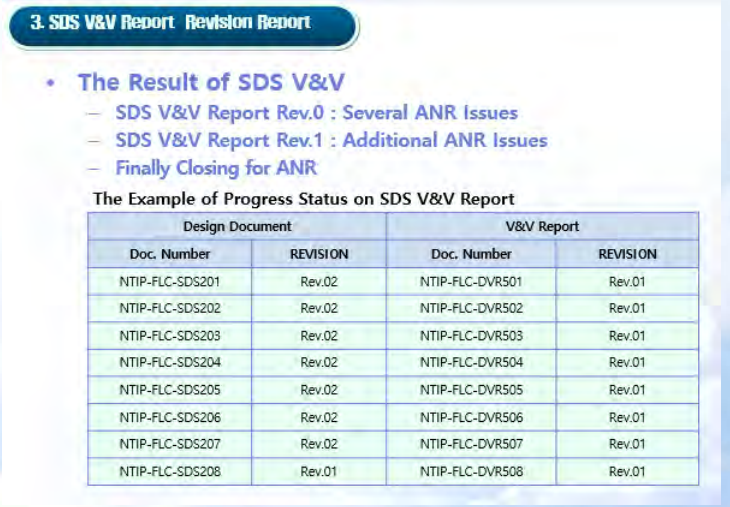
SRS/SDS V&V Report [2]

2. SRS V&V Report Revision Report

- The Results of SRS V&V
  - SRS V&V보고서 Rev.0 : Several ANR Issues
  - SRS V&V보고서 Rev.1 : Additional ANR Issues
  - Finally Closing for ANR

The Example of Progress Status on SRS V&V Report

Design Document		V&V Report	
Doc. Number	REVISION	Doc. Number	REVISION
NTIP-FLC-SRS201	Rev.02	NTIP-FLC-RVR501	Rev.01
NTIP-FLC-SRS202	Rev.02	NTIP-FLC-RVR502	Rev.01
NTIP-FLC-SRS203	Rev.02	NTIP-FLC-RVR503	Rev.01
NTIP-FLC-SRS204	Rev.02	NTIP-FLC-RVR504	Rev.01
NTIP-FLC-SRS205	Rev.02	NTIP-FLC-RVR505	Rev.01
NTIP-FLC-SRS206	Rev.02	NTIP-FLC-RVR506	Rev.01
NTIP-FLC-SRS207	Rev.02	NTIP-FLC-RVR507	Rev.01
NTIP-FLC-SRS208	Rev.01	NTIP-FLC-RVR508	Rev.01



3. SDS V&V Report Revision Report

- The Result of SDS V&V
  - SDS V&V Report Rev.0 : Several ANR Issues
  - SDS V&V Report Rev.1 : Additional ANR Issues
  - Finally Closing for ANR

The Example of Progress Status on SDS V&V Report

Design Document		V&V Report	
Doc. Number	REVISION	Doc. Number	REVISION
NTIP-FLC-SDS201	Rev.02	NTIP-FLC-DVR501	Rev.01
NTIP-FLC-SDS202	Rev.02	NTIP-FLC-DVR502	Rev.01
NTIP-FLC-SDS203	Rev.02	NTIP-FLC-DVR503	Rev.01
NTIP-FLC-SDS204	Rev.02	NTIP-FLC-DVR504	Rev.01
NTIP-FLC-SDS205	Rev.02	NTIP-FLC-DVR505	Rev.01
NTIP-FLC-SDS206	Rev.02	NTIP-FLC-DVR506	Rev.01
NTIP-FLC-SDS207	Rev.02	NTIP-FLC-DVR507	Rev.01
NTIP-FLC-SDS208	Rev.01	NTIP-FLC-DVR508	Rev.01

Code V&V Report

1. V&V Method and Criteria

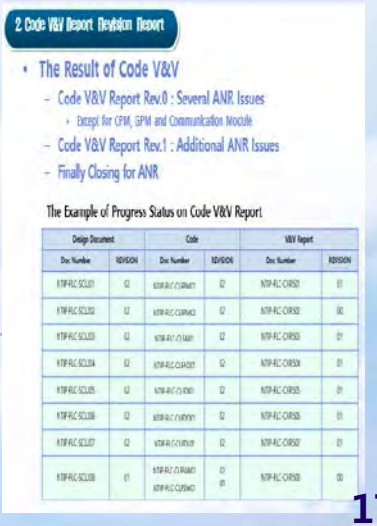
- SRS Criteria Compiling
  - IEEE Std. 1012 based Quality Attributes Measurement between Source Code and Implementation Specification
  - NUREG 0800 Chapter 7/BTP-14 Acceptable Criteria
    - Licensing Suitability.
  - NUREG/CR-7006[1] 기Code Inspection based on Coding Guideline

IEEE Std 1012 Quality Attributes

Traceability Analysis	Source code and source code documentation evaluation	Interface Analysis
Correctness	Correctness	Correctness
Consistency	Consistency	Consistency
Completeness	Completeness	Completeness
	Accuracy	Accuracy
	Readability	Testability
	Testability	

NUREG/CR-7006 Quality Attributes

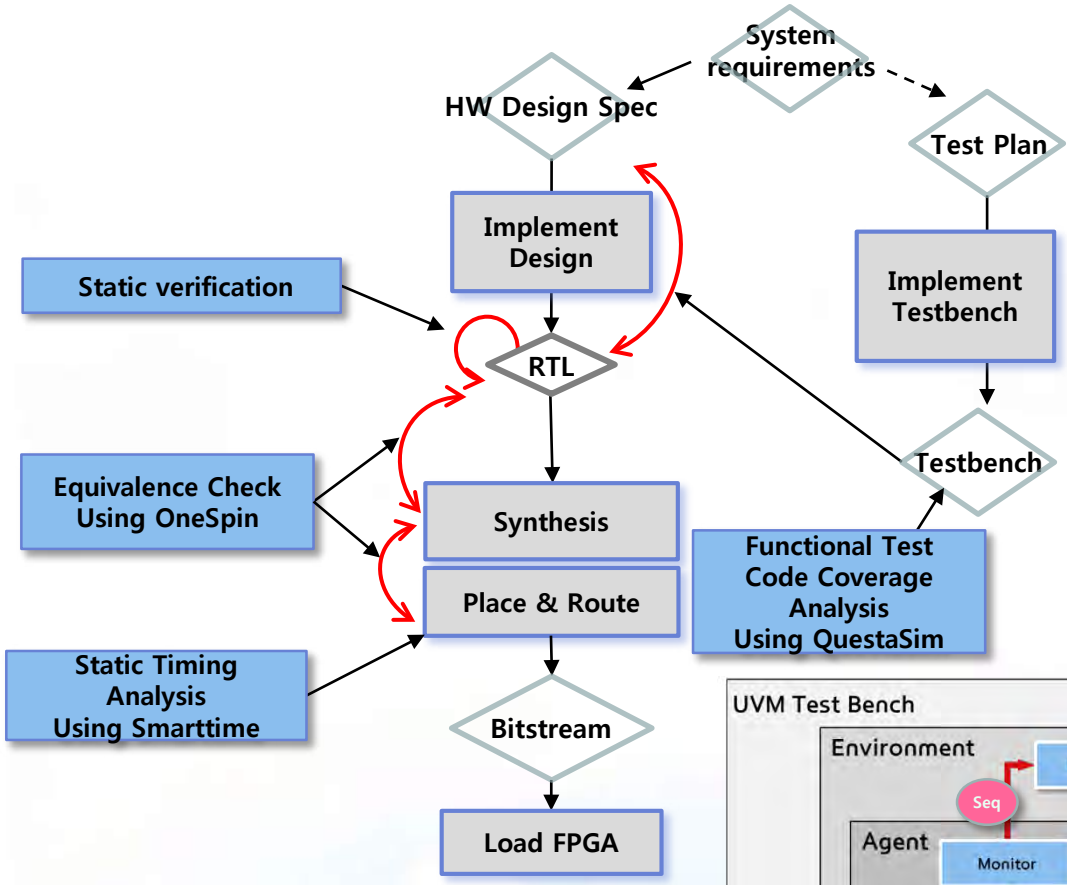
Quality attributes
Reliability
Robustness
Traceability
Maintainability



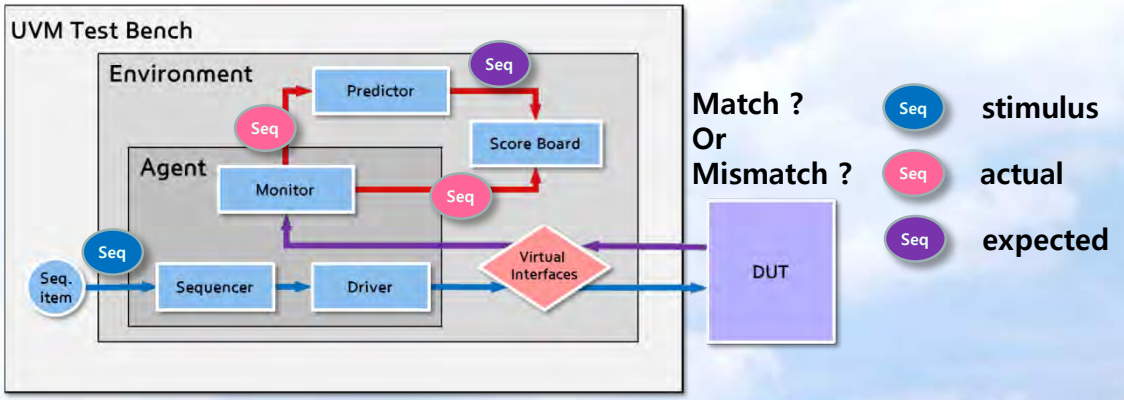
1) FAM-01NUREG CR-7006 : Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems

Component Test

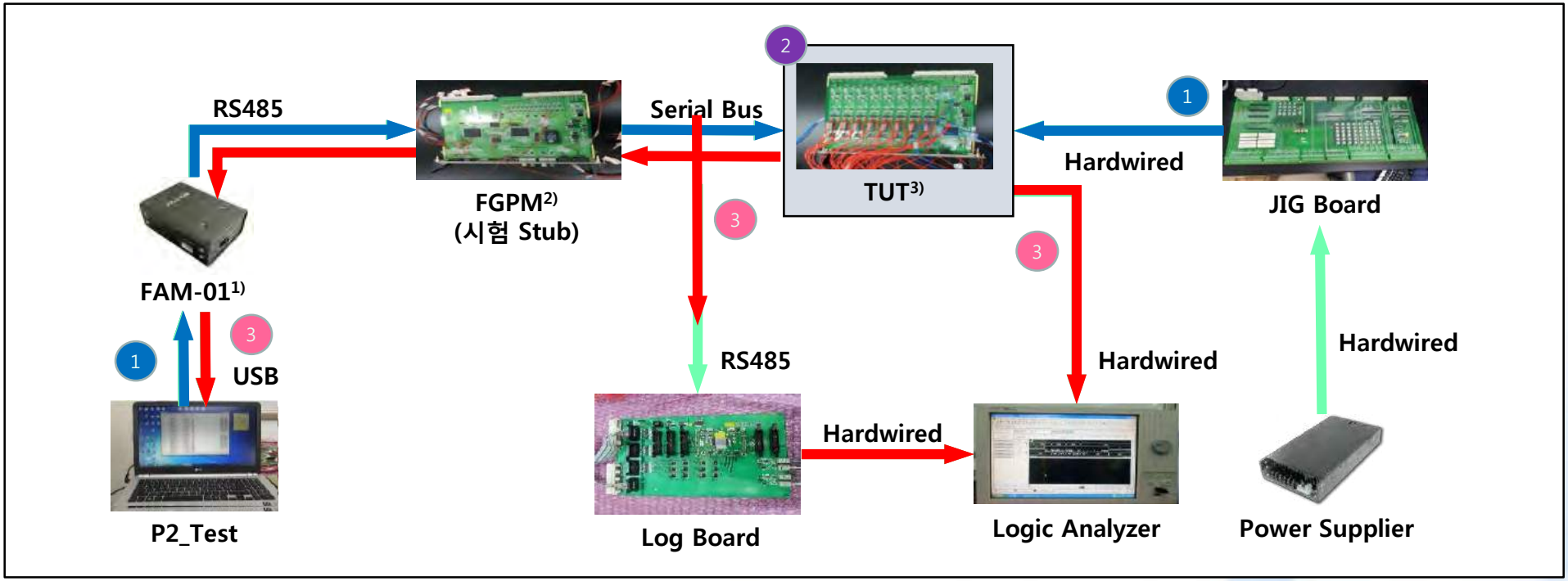
Component Test Procedure



No	Module Name	Signal Name	Expected Output	Actual Output	Pass/Fail	TER No.	Remark
1	clfdi01_top	DGEN	1	1	☑Pass/☐Fail		
2	clfdi01_top	DIAGSCK	0	0	☑Pass/☐Fail		
3	clfdi01_top	DIAGLCK	0	0	☑Pass/☐Fail		
4	clfdi01_top	DIAGSDO	0	0	☑Pass/☐Fail		
5	clfdi01_top	STEN	0	0	☑Pass/☐Fail		
6	clfdi01_top	SRXD	1111	1111	☑Pass/☐Fail		
7	clfdi01_top	LED_RUNP	0	0	☑Pass/☐Fail		
8	clfdi01_top	LED_RUNN	0	1	☐Pass/☑Fail	TER-001-NTIP-FLC-CTR505,Rev1	
9	clfdi01_top	LED_FLTP	0	0	☑Pass/☐Fail		
10	clfdi01_top	LED_FLTN	0	0	☑Pass/☐Fail		
11	clfdi01_top	LED_ST0P	0	0	☑Pass/☐Fail		
12	clfdi01_top	LED_ST0N	0	0	☑Pass/☐Fail		

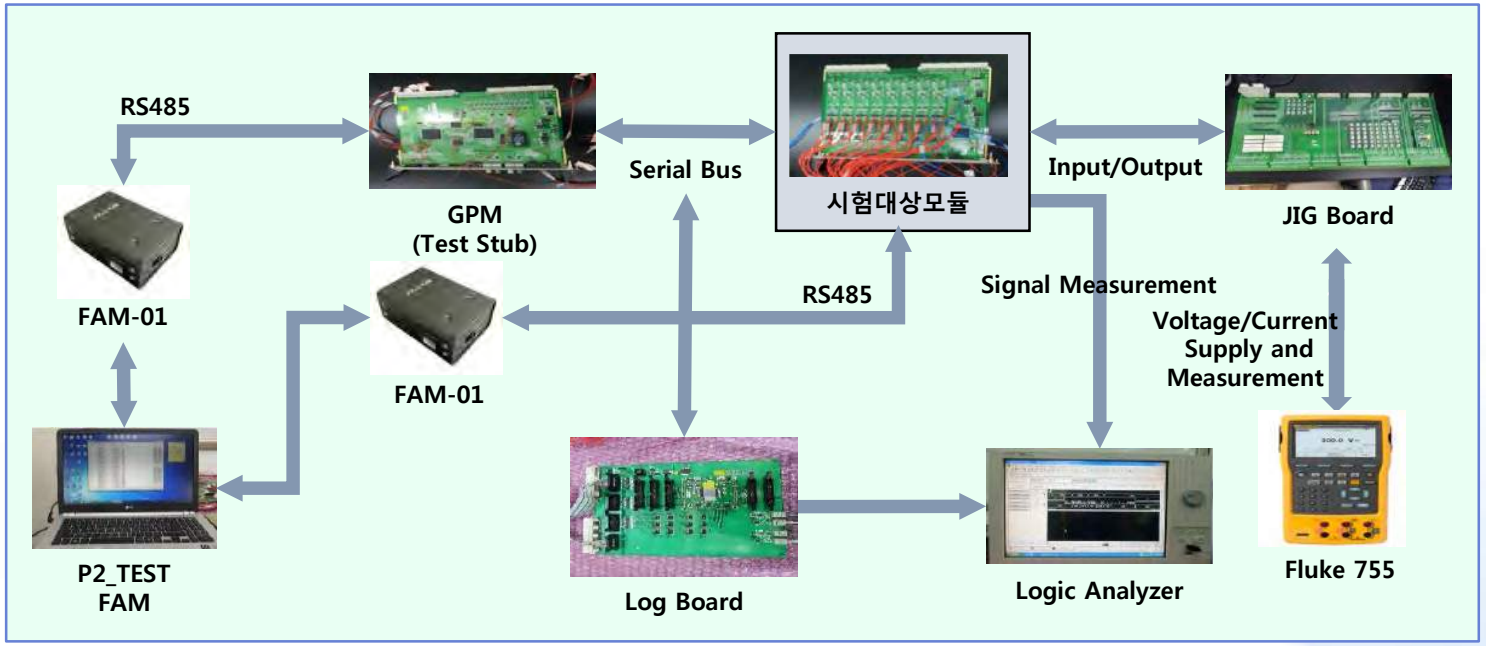


Integration Test[1]



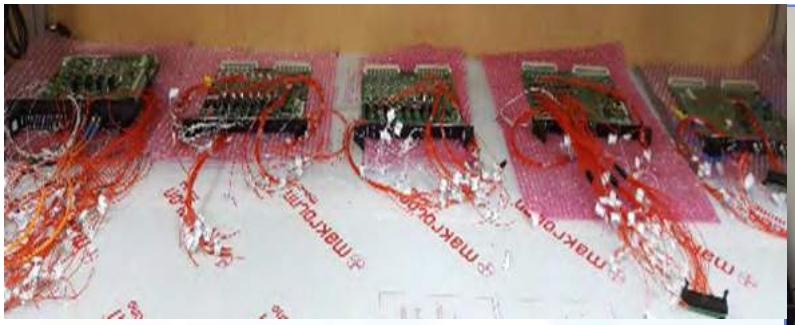
1. Test Data Input from P2_Test Software and JIG Board
2. Test Execution under Test Conditions with Test Data
3. Monitoring through JIG Board and Logic Analyzer

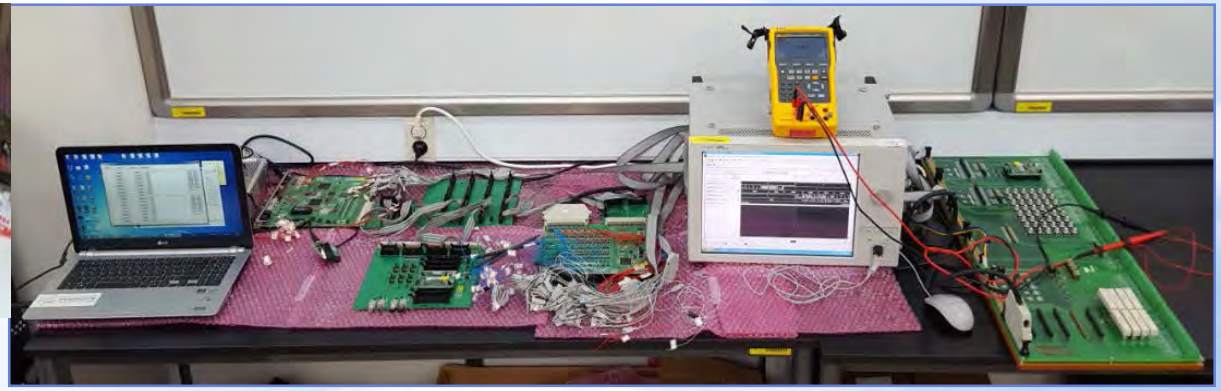
Integration Test[2]



◄ Test Execution Flow

QA Audit DEMO





Real Target Boards► Integration Test Environment

Integration Test[3]

Integration Test

Test Feature: Receiving from Initial Diagnostics Result(Data Frame)

- Check for Receiving from Initial Diagnostics Result(Data Frame) and it's Display status LED.

Test Case: Initial Diagnostics Result Check and LED Check

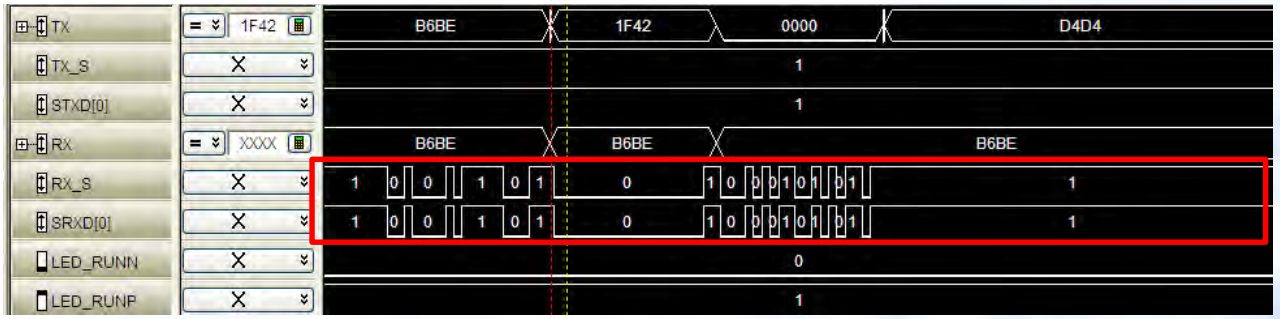
1) Test Input

No	Name	Value	Description
1	BUS_ID	0	Selection of Bus
2	SET_USE_CH	0xFF	Activation for Channel
3	SET_OP_DIAG	0xFF	Activation for Diagnostics

2) Expected Value

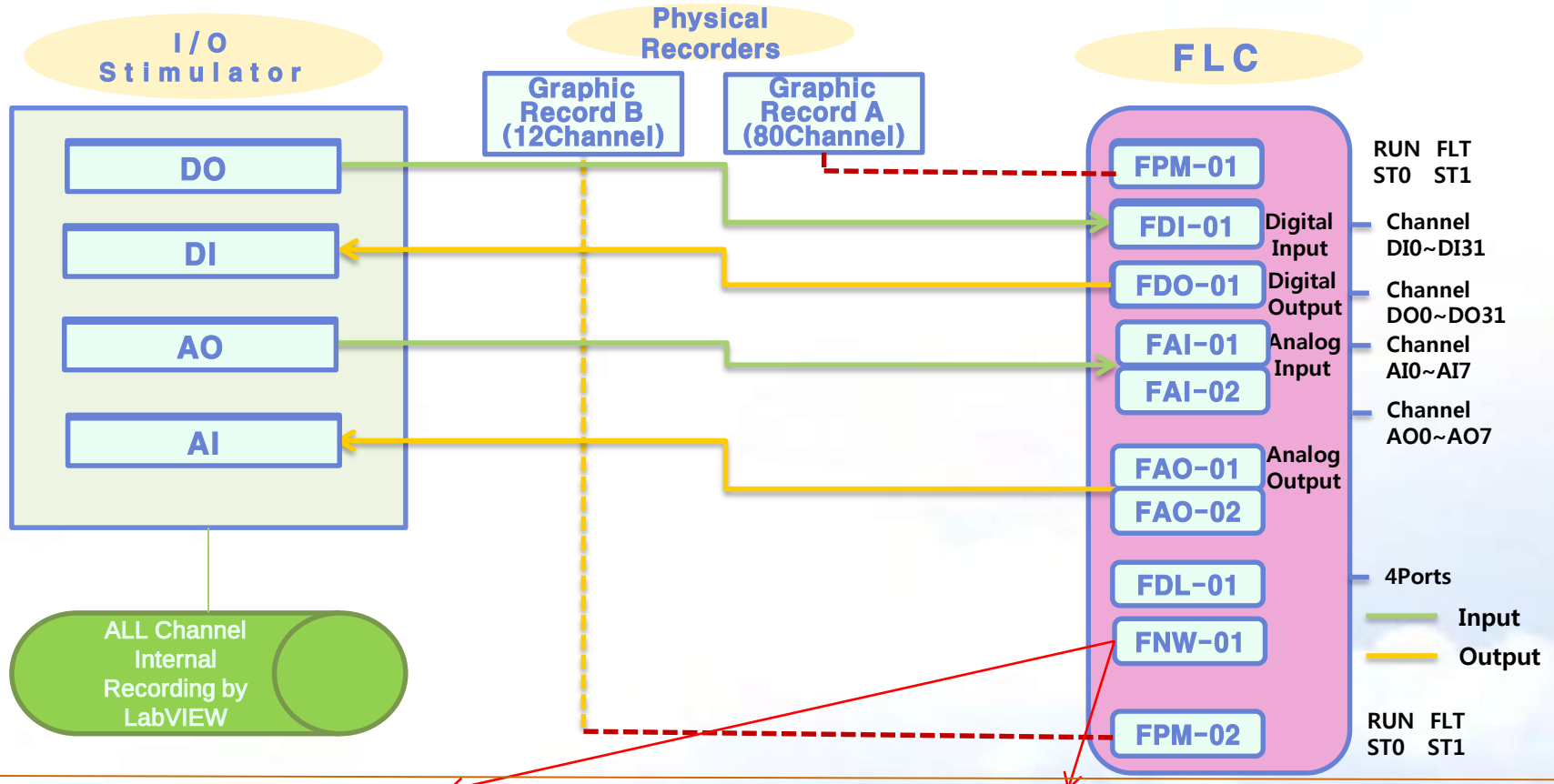
No	Name	Expected Output	Description
1	Slot ID	1f	Slot ID
2	RUN LED	Green	LED Color (Normal Operation)
3	LED_RUNP	0	RUN LED Operation Control (Normal: 0, Process Voltage Error : 1)
4	LED_RUNN	1	

3) Test Output (Logic Analysis)

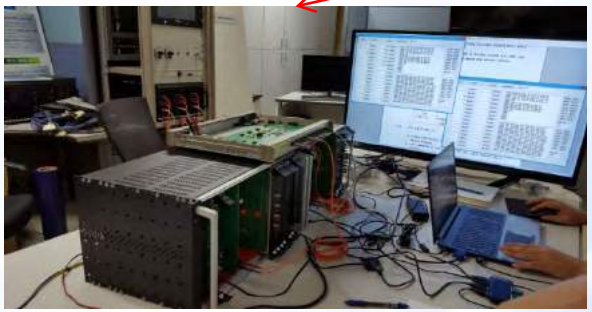


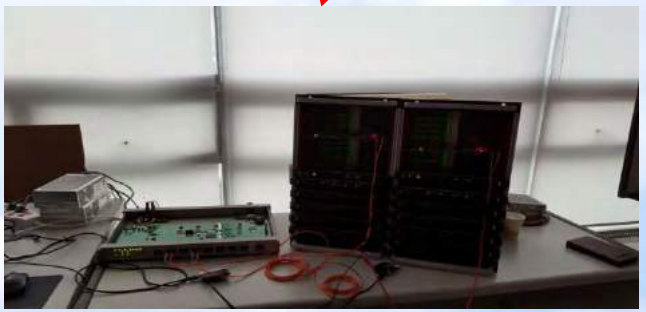
Name	Expected Output	Actual Output	Pass/Fail
Slot ID	1f	1f	Pass
LED_RUNP	0	1	Fail
LED_RUNN	1	0	Fail

Independent Testing Platform : Configuration of FPAG based Logic Controller



Switching Test



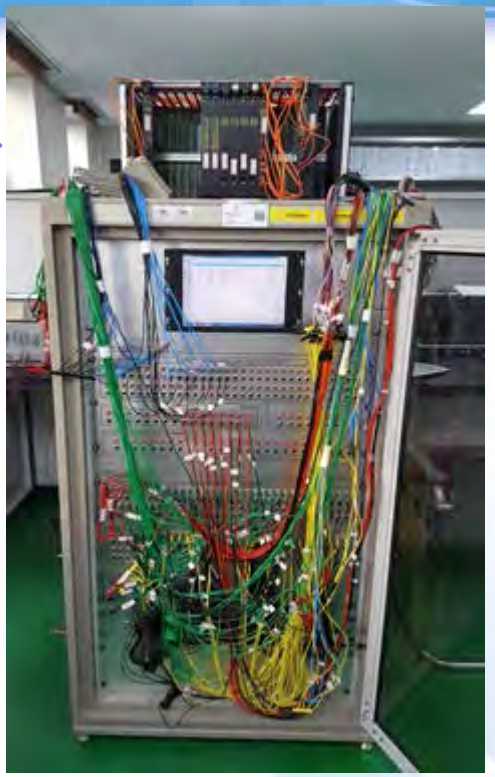


Functional Test
Sending/Receiving

Testing Scenario

Integration Test

Target FLC



System Test

DEMO

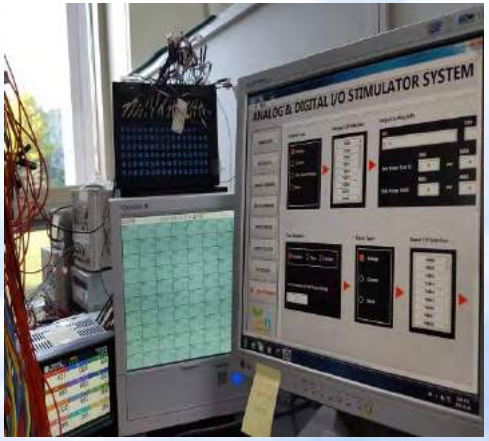
Status Monitoring Screen

1. I/O Stimulator Platform Qualification
   - Y=aX Linear Function, 10,000 test case, Full Scale

3. Pre-Qualification by Manual
   - Fluke 754
   - 1st REC, 2nd REC

4. Scenario based Input/Output Automatic Test
   - FAI-> Internal Bus->FPM01-> FDL-> FAO
   - FDI-> Internal Bus->FPM01-> FDL-> FDO
   - FAI-> Internal Bus->FPM01-> FDL-> FDO (cross)
   - FDI->Internal Bus-> FPM01-> FDL-> FAO
     - (Triangle : 0-Rising-Falling-0 : 10,000 Test Case, 200ms, 01.%)

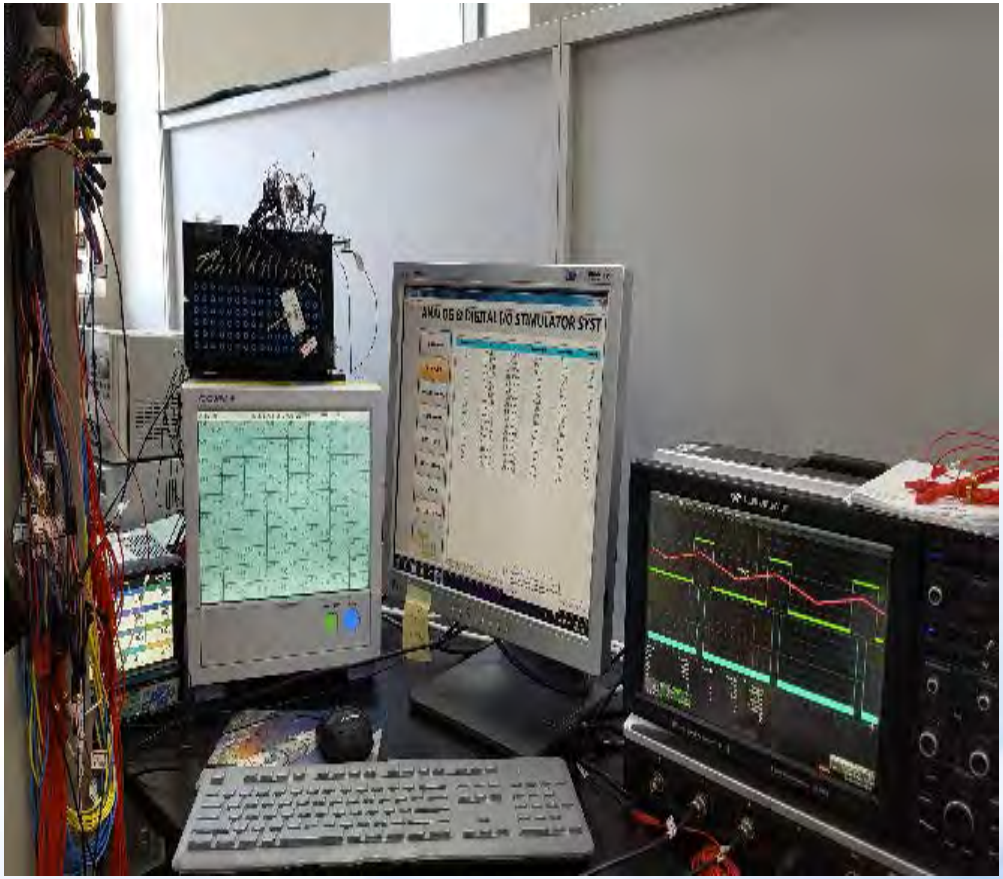
5. Test Result and Analysis



1st REC
2nd REC

System Test for FLC

Target FLC

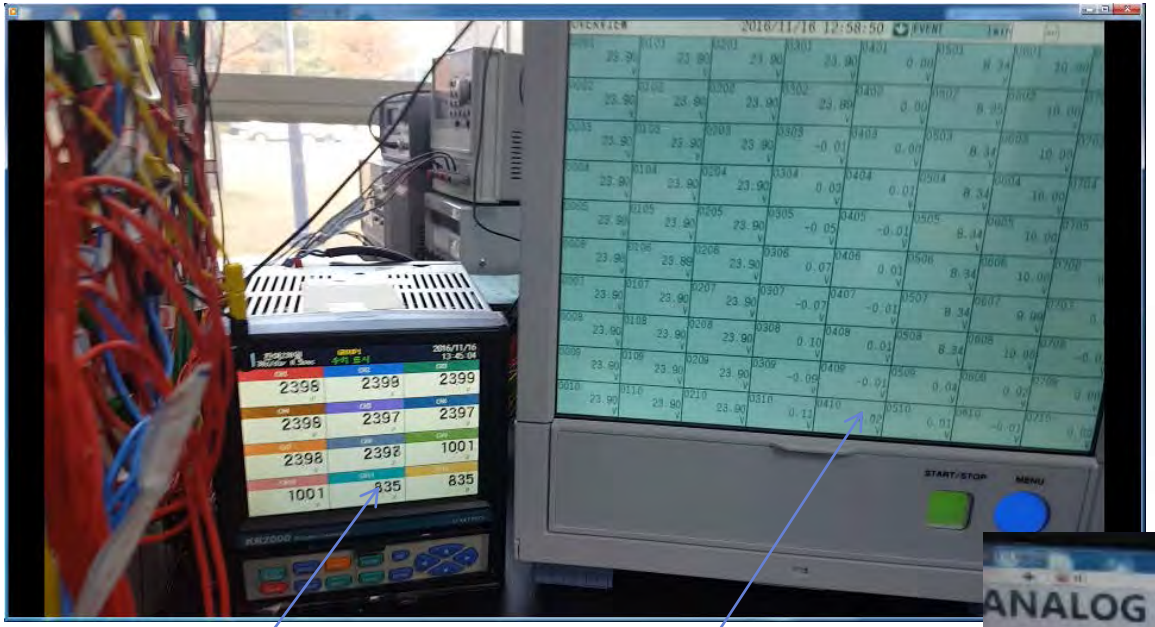


Automatic Signal Generator
- Manual Test
- Automatic Test by initiating Manual

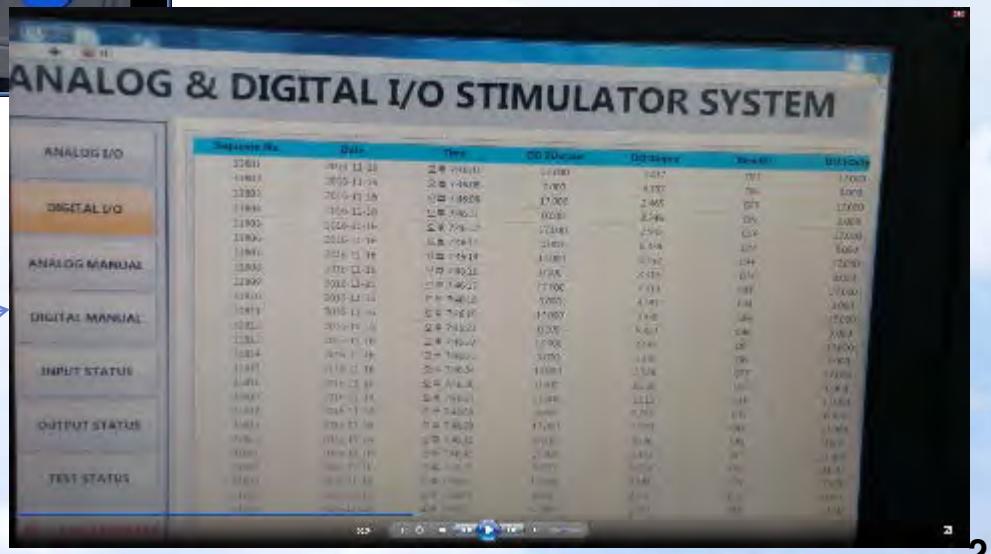
Test Result
- Pass/Fail
- Real-time Performance

Automatic Test Results (Sample)

External Measurement



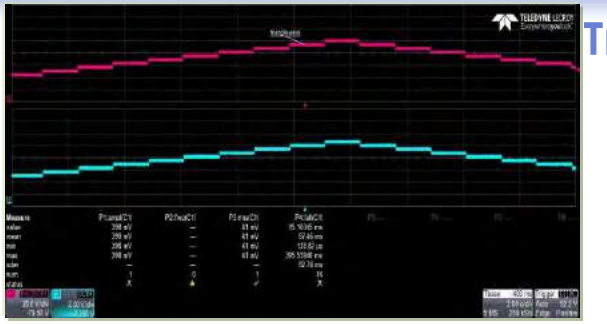
Internal Measurement :
Pass/Fail Decision by timing parameter



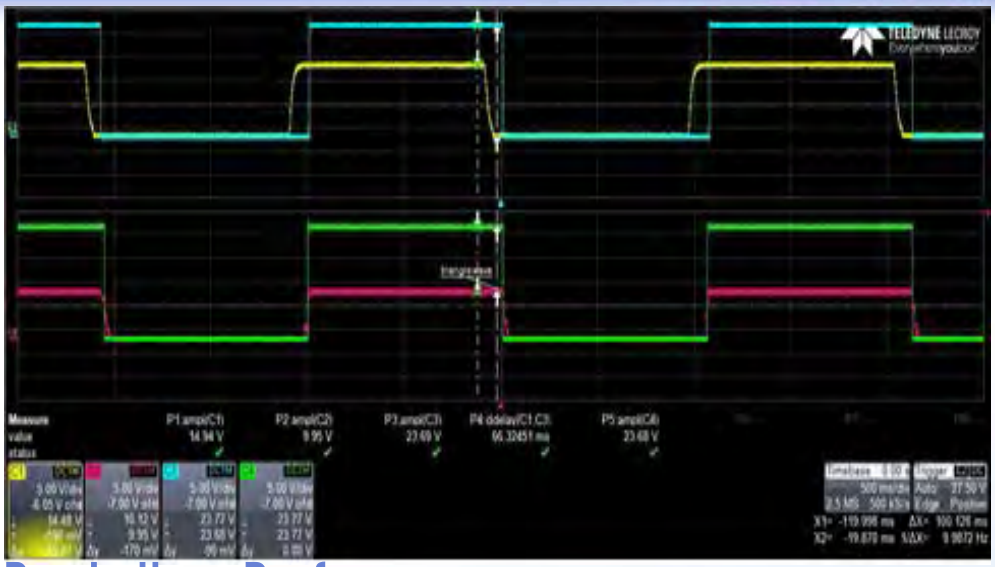
FPM-02

FPM-01

Test Results(Real-time)

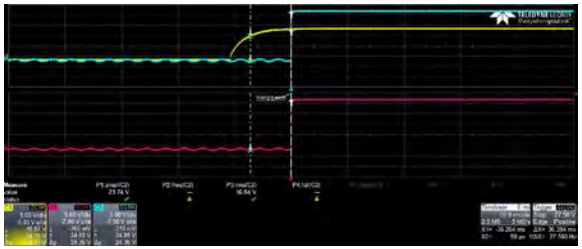


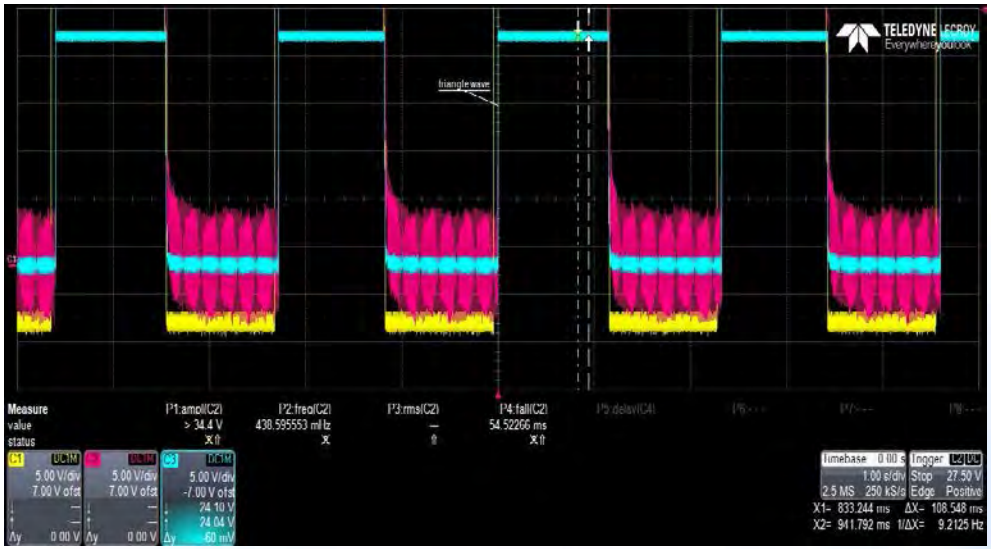
Triangle Wave



Real-time Performance

Conversion Time Trend (Cross)

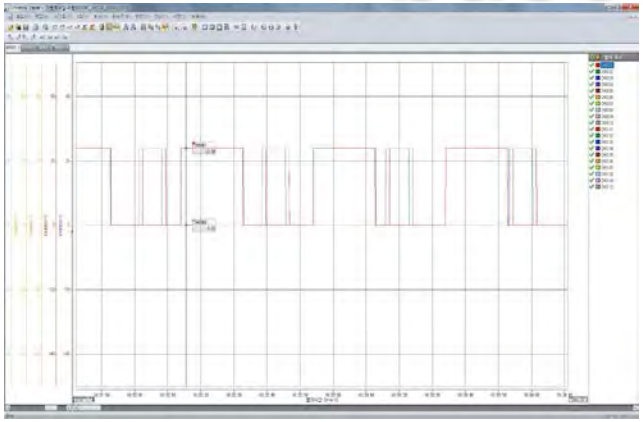




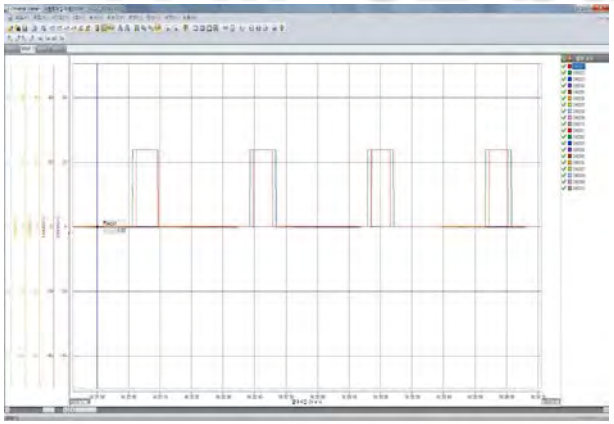
Precision

Timing Analysis

Static Analysis of Test Result : FPM-01 based & FPM-02 based



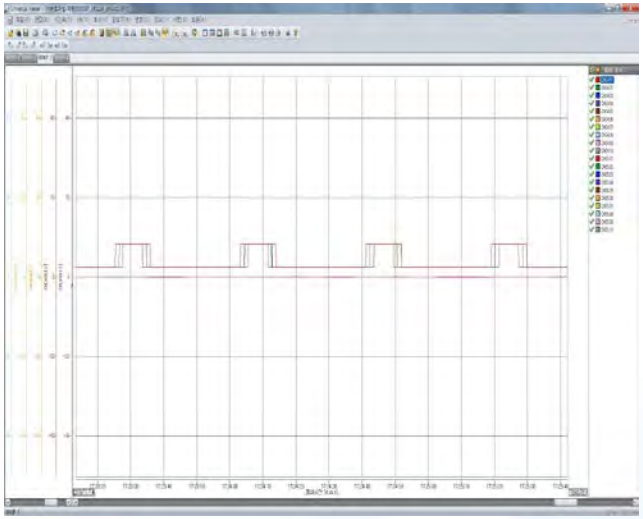
FAI->FDL->FDO, (FDI-> FDL-> FDO)



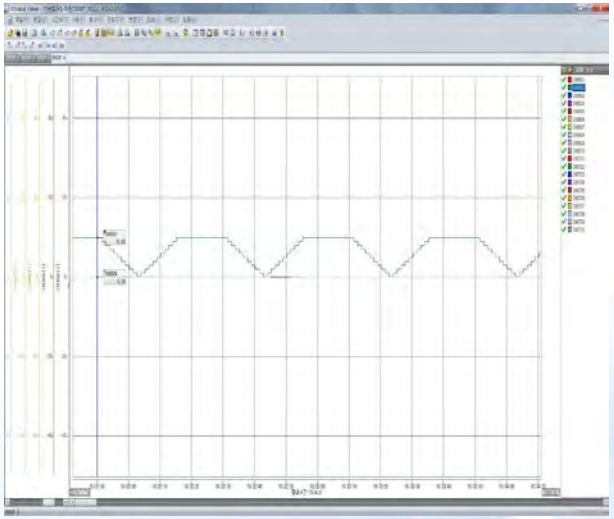
FDI-> FDL-> FDO

FPM-01

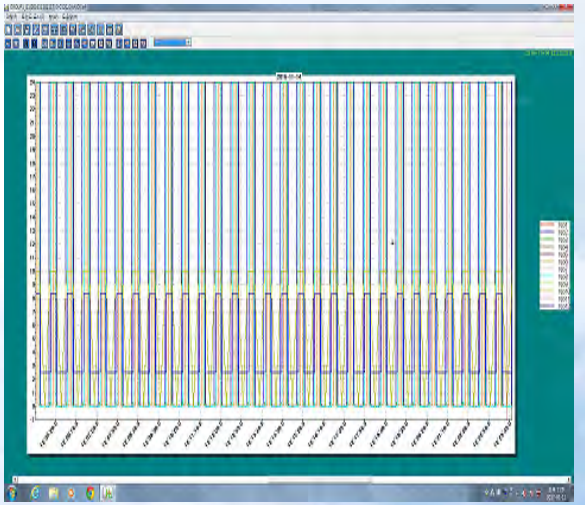
FPM-02



FDI-> FDL-> FAO



FAI-> FDL-> FAO



All(FAI-> FDL-> FDO,FDI-> FDL-> FDO, FDI-> FDL-> FAO, FAI-> FDL-> FAO)

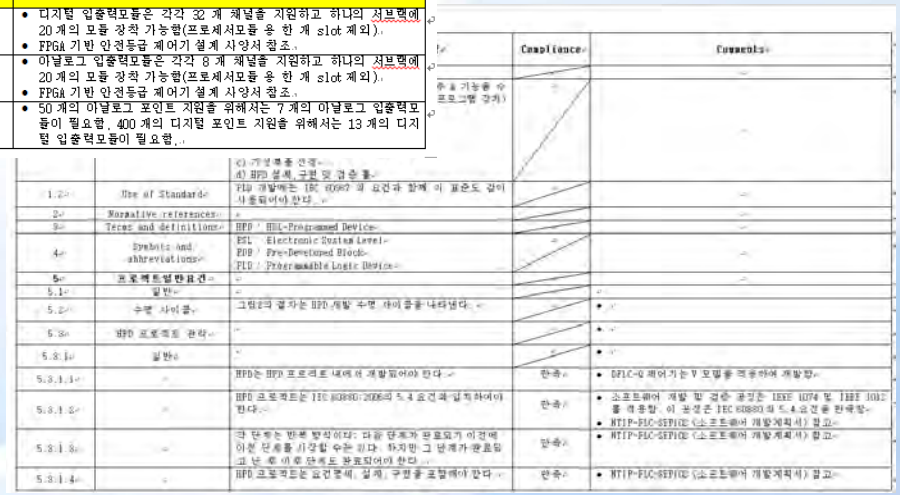
Licensing Suitability : Compliance Check

■ 부록 A: IEEE Std 7-4.3.2-2003 만족여부

Section	Title	IEEE Std 7-4.3.2-2003 요건 요약	Compliance	Comments
1.	Scope		해당 없음	
2.	References		해당 없음	
3.	Keyword		해당 없음	
4.	안전계통 설계기준	IEEE std 603-1998의 해당요건을 만족해야 한다.	해당 없음	
5.	안전계통 기준		해당 없음	
5.1	단일고장기준	IEEE std 603-1998의 해당요건을 만족해야 한다.	해당 없음	
5.2	보호조치완결	IEEE std 603-1998의 해당요건을 만족해야 한다.	해당 없음	
5.3	품질	하드웨어 품질은 IEEE std 603-1998측 만족하고 소프트웨어 품질은 IEEE/EIA std 12207.0-19	해당 없음	
5.3.1	소프트웨어 개발	1. 컴퓨터 소프트웨어는 IEEE/EIA 1 만족하는 승인된 소프트웨어 품질 발, 수정 또는 승인되어야 한다.		
		2. 소프트웨어 품질보증계획에는 컴퓨터에 내재되어 있는 모든 프로며, 소프트웨어 품질보증 계획 제 60880(1986-09) 및 IEEE Std 730 있다.		
5.3.1.1	소프트웨어 품질측정	소프트웨어 품질 측정이 이용될 때 별로 특성들이 고려되어야 한다.		
		- 정확성/완결성 (요건단계)		
		- 요건의 만족 (설계단계)		
		- 설계의 만족 (구현단계)		

■ 부록 B: EPRI TR-107330 만족여부

Section	요건	EPRI TR-107330 요건 요약	Compliance	Comments
1.	Scope			
2.	Definitions, Abbreviations, Acronyms			
3.	Reference			
4.	System Requirements			
4.1	Overview of Performance Basis			
4.2	기능요건			
4.2.1	일반 기능요건			
4.2.1.A	응답시간	응답시간은 100 msec 이하이어야 하고 다음 사항을 포함하여야 함. 1. 필터링 시간. 2. 입력모듈에서의 디지털 신호 변환 시간. 3. Main processor가 PLC 버스를 통하여 입력 값을 습득하는데 걸리는 시간. 4. 2000개 정도의 단순 로직요소를 포함하는 응용프로그램의 2번 스캔에 소요되는 시간. 5. Main Processor가 PLC 버스를 통하여 출력모듈로 데이터를 전송하는 시간. 6. 출력모듈이 버스를 통하여 수신된 디지털 데이터를 해당하는 출력신호레벨로 변환하는 시간. 7. 이중화 프로세서의 동기화, 프로세서간의 통신 관련 알고리듬의 실행을 포함하는 이중화 기능 수행 및 자기진단에 필요한 최대시간.	만족	• 아날로그 입출력, 디지털 입출력에 대한 응답 시간은 50ms 이하로 요건을 만족함. • 데이터링크 통신을 포함한 아날로그 입출력, 디지털 입출력에 대한 응답 시간은 100ms 이하로 요건을 만족함. • FPGA 기반 안전등급 제어기 설계 사양서 참조. • FPGA 기반 안전등급 제어기 기능 및 성능 시험보고서 참조. (예외사항) 1. 이중화 프로세서는 사양에 적용하지 않음.
4.2.1.B	Discrete I/O수량	PLC 는 최소 400 포인트의 discrete I/O 를 수용할 수 있어야 함.	만족	• 디지털 입출력모듈은 각각 32 개 채널을 지원하고 하나의 서브랙에 20 개의 모듈 장착 가능함(프로세서모듈 용 한 개 slot 제외). • FPGA 기반 안전등급 제어기 설계 사양서 참조.
4.2.1.C	Analog I/O 수량	PLC 는 최소 100 포인트의 analog I/O 를 수용할 수 있어야 함.	만족	• 아날로그 입출력모듈은 각각 8 개 채널을 지원하고 하나의 서브랙에 20 개의 모듈 장착 가능함(프로세서모듈 용 한 개 slot 제외). • FPGA 기반 안전등급 제어기 설계 사양서 참조.
4.2.1.D	조합 I/O 수량	PLC 는 최소 50 개의 analog 포인트와 400 개의 discrete I/O 포인트를 수용 할 수 있어야 함.	만족	• 50 개의 아날로그 포인트 지원을 위해서는 7 개의 아날로그 입출력모듈이 필요함. 400 개의 디지털 포인트 지원을 위해서는 13 개의 디지털 입출력모듈이 필요함.



Conclusions

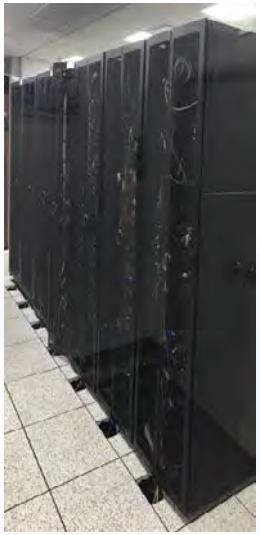
- QA/SQA/SCM
- COTS Dedication/Tool Quaity Evaluation
- SA
- SVV : Independent Testing
  - Automatic Testing!!!

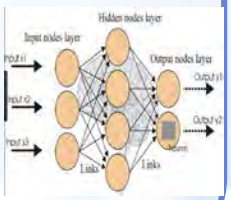
Future Plans

- Sensors
  - Press
  - Level
  - Temp
    - RTD
    - Bimeta
  - Relay

Clouds/Cluster

IoT+AI





Producing Verification Data