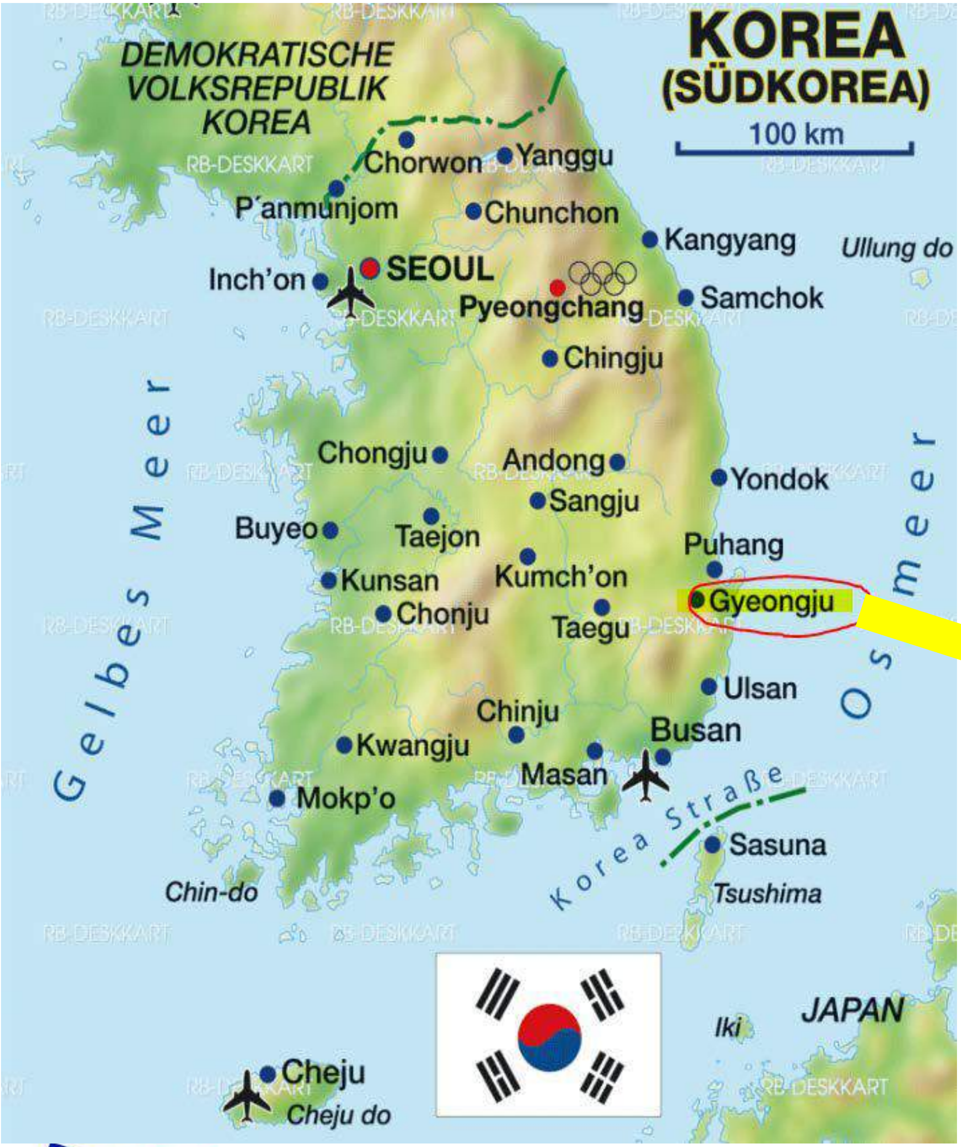
9th International Workshop on Application of FPGA in NPP,

hosted by EDF SEPTEN in cooperation with the IAEA and SunPort SA

Schedule for the 10th International Workshop on Application of FPGA in NPP
2018, November 22~24, Gyeongju in Korea



November 2017

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				2	3	4
5				9	10	11
12				16	17	18
19	20	21	22 10th FPGA Workshop	23	24	25
26 International Symposium on Future I&C for NPPs	27	28	29	30		

Doosan Heavy Industries & Construction

DI&C Technology to upgrade the Analog System with the Digital equipment in Operating NPPs

Nam Chae Ho

Lyon, France

Oct 3, 2016

9th International Workshop on Application of FPGA in NPP,
hosted by EDF SEPTEN in cooperation with the IAEA and SunPort SA.

Table of Contents

1. Introduction

. Background

2. DI&C Solution

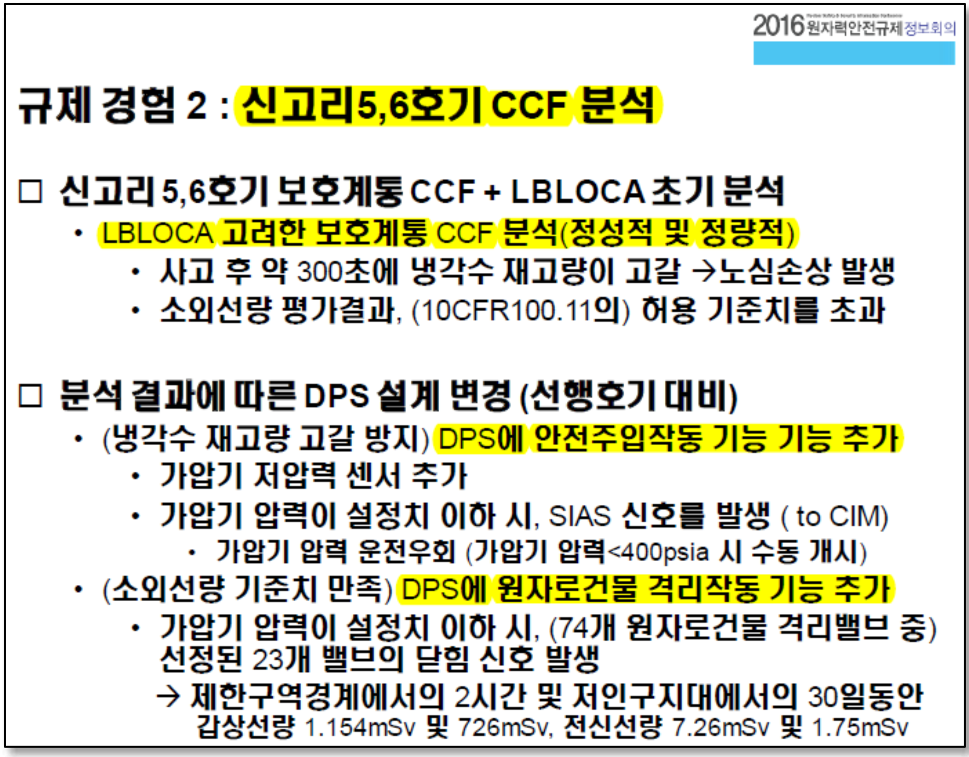
. CCF – different person, organization & platform…
. SPV – redundancy & combination architecture
. Cyber security – critical vulnerability, combining
White & Black list technology, etc.
. Class 1E FPGA based Platform – V&V, EQ

3. Additional suggestion

. Code Simulator is good for validation of newly developed system

I. Introduction
- Background - CCF

- **CCF Requirements are continuously being increased to make sure safety & reliability of NPP**
  - ✓ ***As the Regulatory body requires the Safety analysis of CCF under LBLOCA***
  - ✓ ***DPS design change requested to add the function of PPS.***



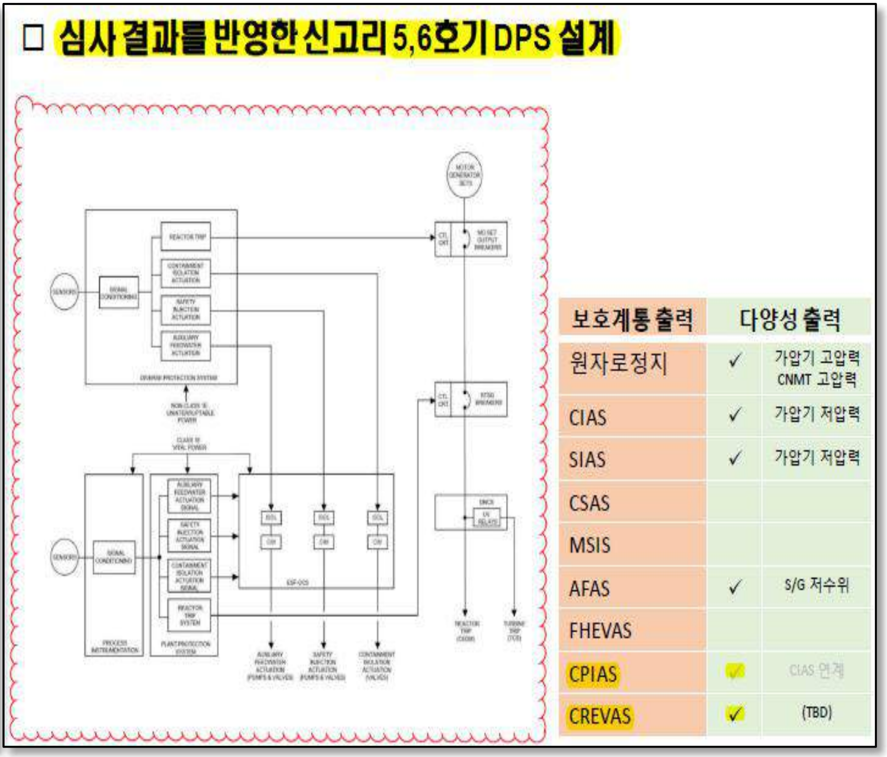
2016 원자력안전규제정보회의

규제 경험 2 : 신고리5,6호기 CCF 분석

□ **신고리 5,6호기 보호계통 CCF + LBLOCA 초기 분석**
- LBLOCA 고려한 보호계통 CCF 분석(정성적 및 정량적)
  - 사고 후 약 300초에 냉각수 재고량이 고갈 →노심손상 발생
  - 소외선량 평가결과, (10CFR100.11의) 허용 기준치를 초과

□ **분석 결과에 따른 DPS 설계 변경 (선행호기 대비)**
- (냉각수 재고량 고갈 방지) DPS에 안전주입작동 기능 기능 추가
  - 가압기 저압력 센서 추가
  - 가압기 압력이 설정치 이하 시, SIAS 신호를 발생 (to CIM)
    - 가압기 압력 운전우회 (가압기 압력<400psia 시 수동 개시)
- (소외선량 기준치 만족) DPS에 원자로건물 격리작동 기능 추가
  - 가압기 압력이 설정치 이하 시, (74개 원자로건물 격리밸브 중) 선정된 23개 밸브의 닫힘 신호 발생

    → 제한구역경계에서의 2시간 및 저인구지대에서의 30일동안 갑상선량 1.154mSv 및 726mSv, 전신선량 7.26mSv 및 1.75mSv



□ **심사 결과를 반영한 신고리 5,6호기 DPS 설계**

MOTOR GENERATOR SETS
CTL CKT
MG SET OUTPUT BREAKERS
REACTOR TRIP
CONTAINMENT ISOLATION ACTUATION
SAFETY INJECTION ACTUATION
AUXILIARY FEEDWATER ACTUATION
SENSORS
SIGNAL CONDITIONING
DIVERSE PROTECTION SYSTEM
CTL CKT
RTSG BREAKERS
NON-CLASS 1E UNINTERRUPTABLE POWER
CLASS 1E VITAL POWER
AUXILIARY FEEDWATER ACTUATION SIGNAL
SAFETY INJECTION ACTUATION SIGNAL
CONTAINMENT ISOLATION ACTUATION SIGNAL
REACTOR TRIP SYSTEM
SENSORS
SIGNAL CONDITIONING
PROCESS INSTRUMENTATION
PLANT PROTECTION SYSTEM
ISOL
CIM
ESF-CCS
UV RELAYS
REACTOR TRIP (CEDM)
TURBINE TRIP (TCS)
AUXILIARY FEEDWATER ACTUATION (PUMPS & VALVES)
SAFETY INJECTION ACTUATION (PUMPS & VALVES)
CONTAINMENT ISOLATION ACTUATION (VALVES)

보호계통 출력	다양성 출력	
원자로정지	✓	가압기 고압력 CNMT 고압력
CIAS	✓	가압기 저압력
SIAS	✓	가압기 저압력
CSAS		
MSIS		
AFAS	✓	S/G 저수위
FHEVAS		
CPIAS	✓	CIAS 연계
CREVAS	✓	(TBD)

I. Introduction

- Background - SPV

- **SPVs are continuously being removed to enhance the reliability of NPP**
  - ***SSPS have still more than 80 SPVs***

Good Practice - Zero SPV CEDMCS

◆ ***After analyzing SPV of CEDMCS, finding 297 SPVs.***

◆ ***Finally, CEDMCS renovated to '0' SPV Systems***

- *Step 1 : Identify – Define the single point vulnerability*
- *Step 2 : Evaluate – Scrutinize all items*
- *Step 3 : Design : Eliminate or mitigate SPVs.*
- *Step 4 : Test – Verify & Validation of all items*

◆ ***Enhance the Maintain & Test Ability***

- *On-line replacement of PCM or Electronic Cards*

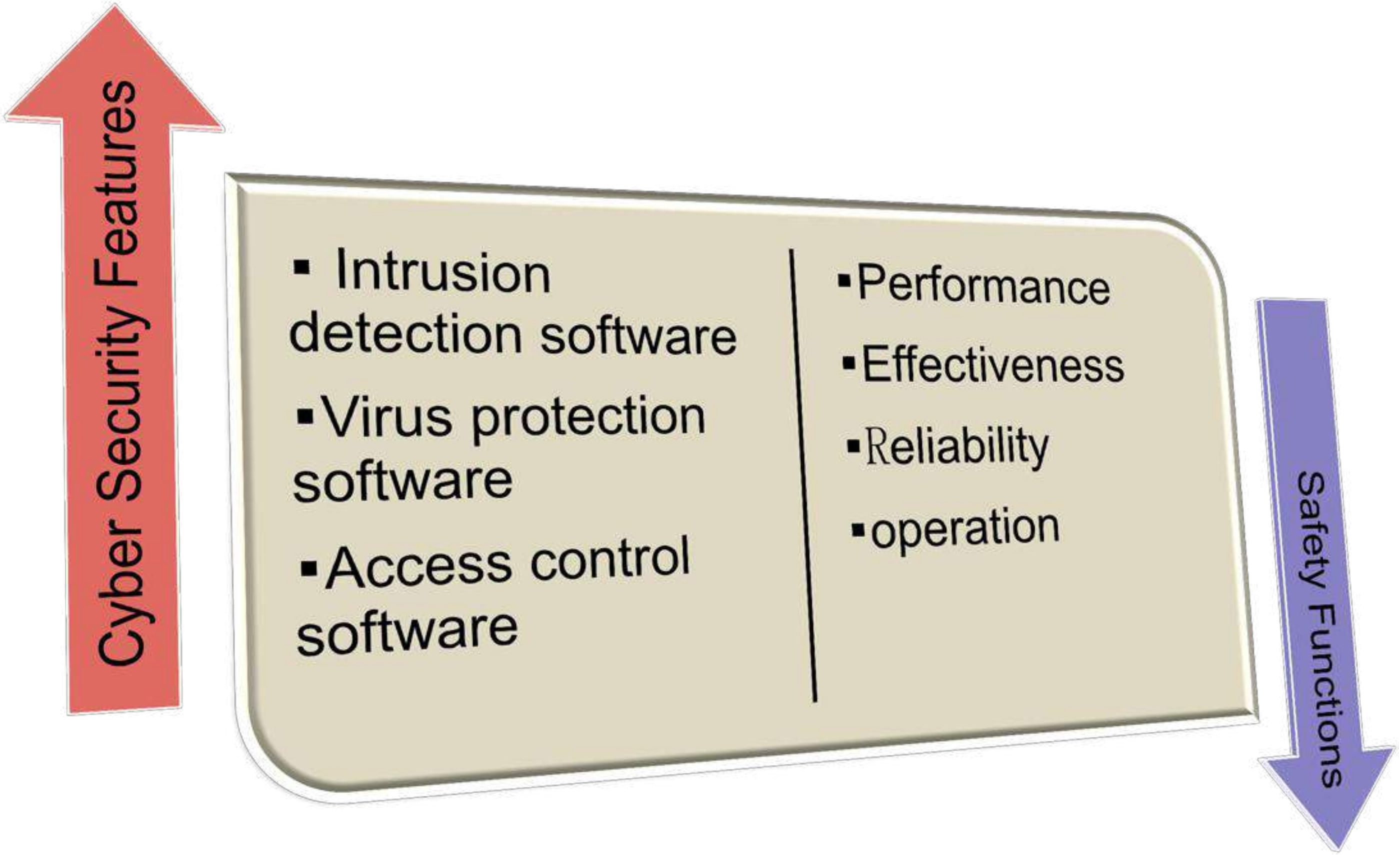
- *Test by CRCS(3-Coil Type) & CEDMCS(4-Coil Type) MMI*

SPV: Single Point Vulnerability

I. Introduction

- Background – Cyber security

- **The Issue of cyber security features & safety functions**
  - ***Conflict between safety functions & cyber security features: Implementation of cybersecurity features shall not adversely impact safety functions.***



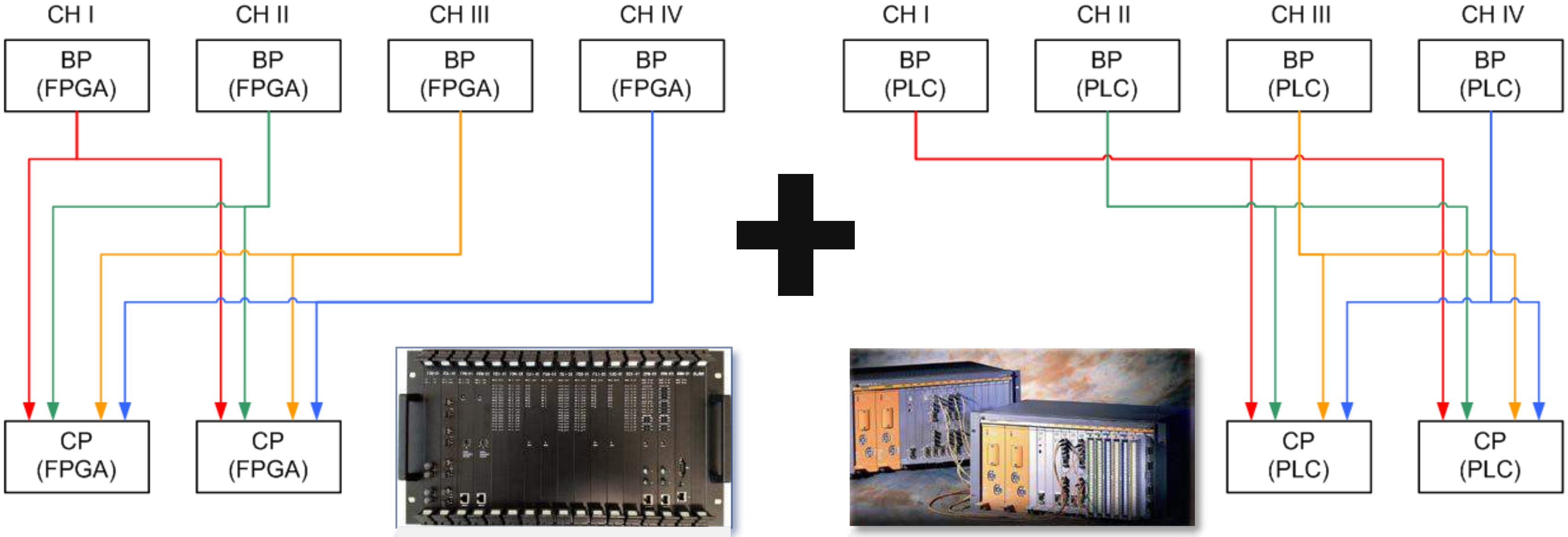
Reference Documents: IEEE Std. 7-4.3.2-2016 5.9.3 Interaction between cyber security features and safety functions

II. DI&C Solution

- Countermeasure for CCF Issues

■ **Different Platform of PPS will resolve the CCF Issues without DPS**

- ✓ ***As is – Class 1E Protection System and Non-Class 1E DPS***
- ✓ ***To be – Class 1E independent Protection System using different platform***
- ✓ ***For example) FPGA based PPS and PLC based PPS are using the same time.***



Doosan FPGA

POSAFE-Q PLC

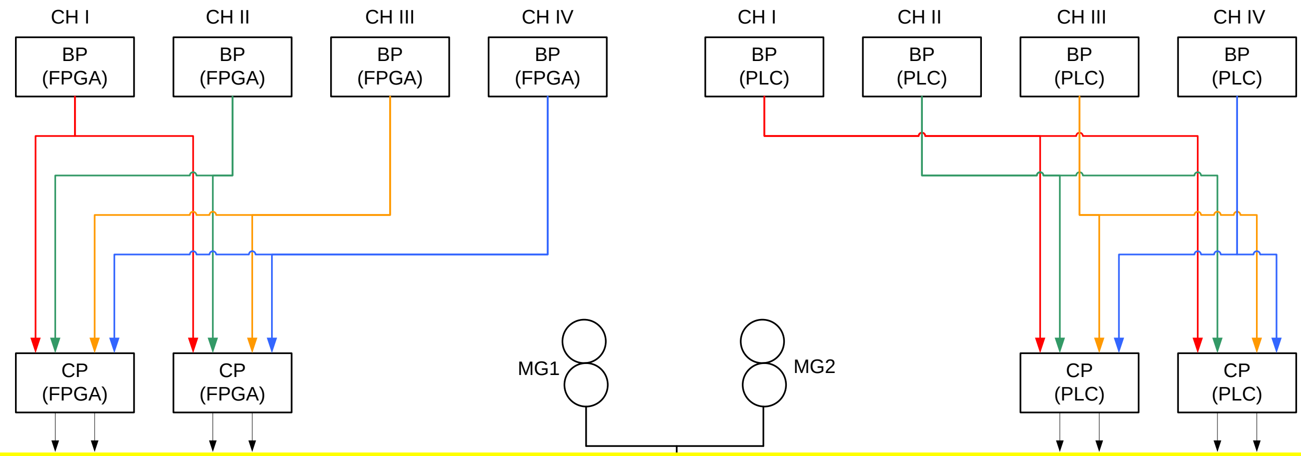
II. DI&C Solution

- Countermeasure for SPV Issues

- **Redundancy & Combination IC eliminate the SPVs of Protection System**

✓ ***As is – Single two train trip logic***

✓ ***To be – Redundant & Combination Trip Initiation Circuit***



Section 1.9 of BTP 7-19 Revision 6 ….. CCF mentioned by Sergio Russomanno today morning^^

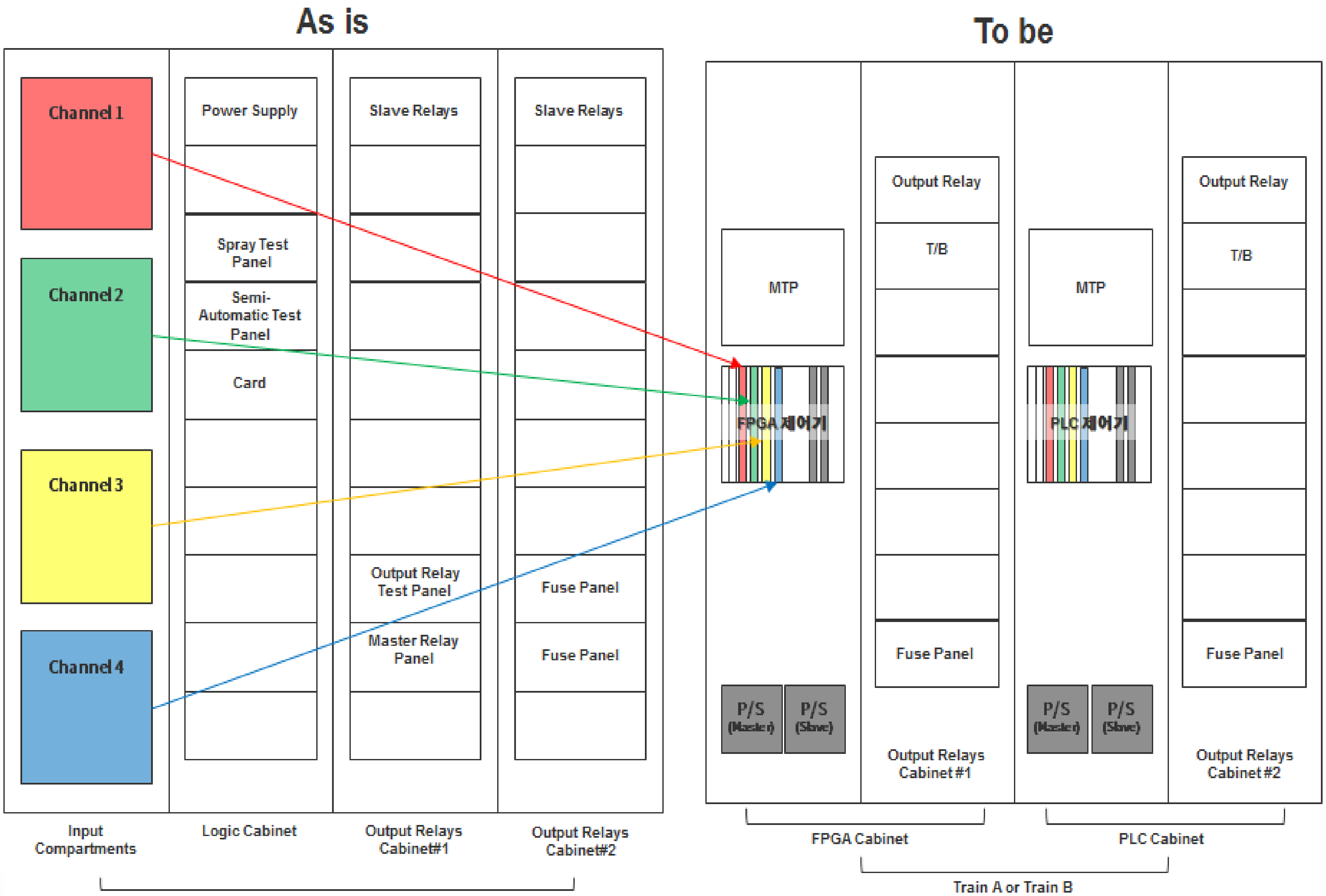
You can see the real solution of CCF in 10th FPGA W/S at Gyeongju

CEDM
(Trip)

II. DI&C Solution

- Countermeasure for CCF & SPVs

Redundant with independent platform architecture for Protection Systems



II. DI&C Solution

- Countermeasure for CCF & SPVs

- **Redundancy & Combination IC remove the SPV and address the CCF**

✓ ***Both independent Platforms & combination trip circuits address both Issues.***

✓ ***Combination Trip Initiate Logic consists of parallel and/or series hardwired with NC and/or NC contact)***

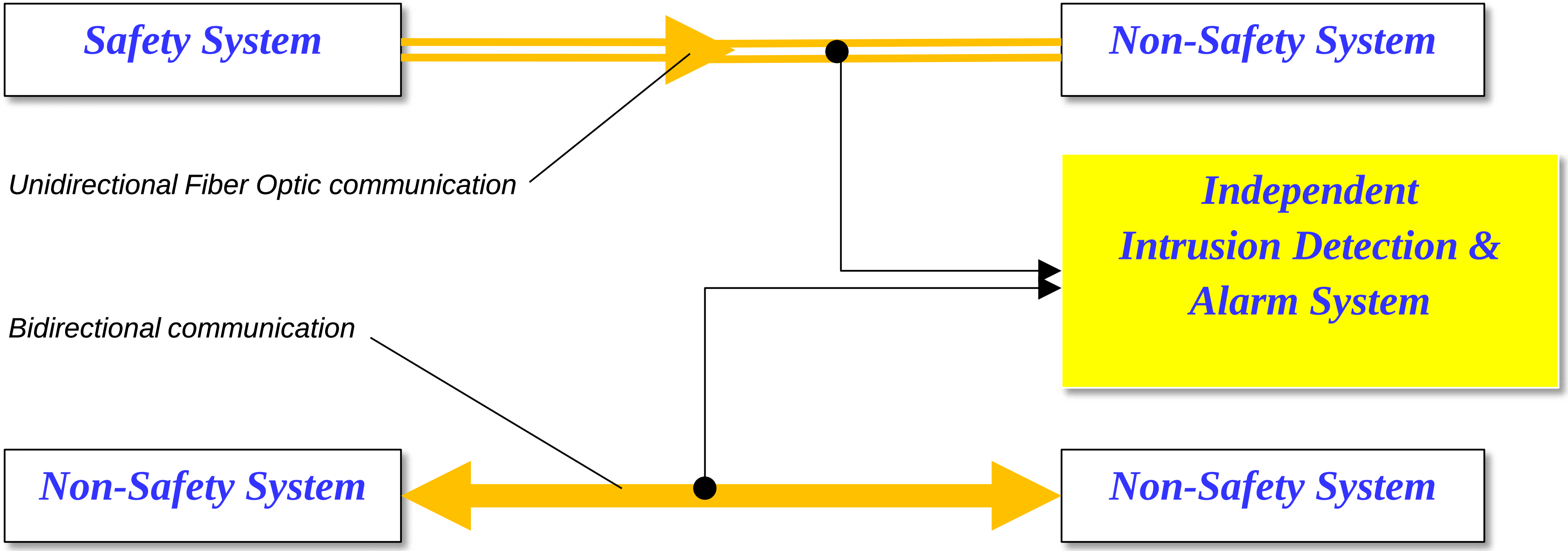
Fail Mode \ Operation Mode		Normal Operation (Operability)	Safety Function (Reliability)
CCF	Open Fail	O	O
	Close Fail	O	O
	Toggle Fail	X	O
SPV	Trip Component	O	O
	Vital Bus Fail	O	O

II. DI&C Solution

- Countermeasure for Cyber Security

Independent Monitoring/Diagnosis of Cyber Attack

must continuously monitor for signs of attack and compromise on all covered devices.
Ex) Monitoring unknown(or un-designed) data packets, unauthorized clients or MAC.



Safety System

Non-Safety System

Unidirectional Fiber Optic communication

Independent Intrusion Detection & Alarm System

Bidirectional communication

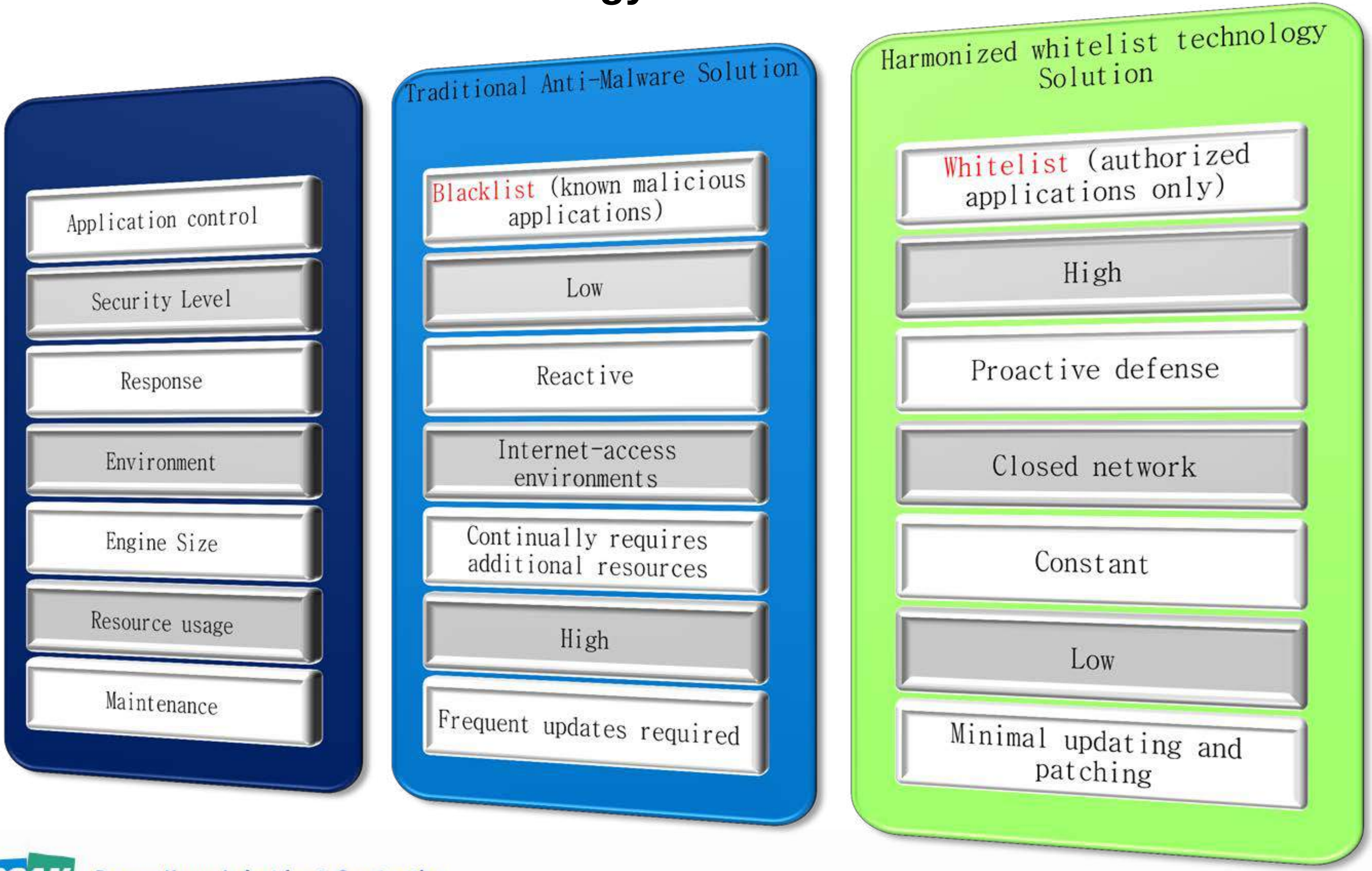
Non-Safety System

Non-Safety System

II. DI&C Solution

- Countermeasure for Cyber Security

Blacklist vs. Whitelist technology



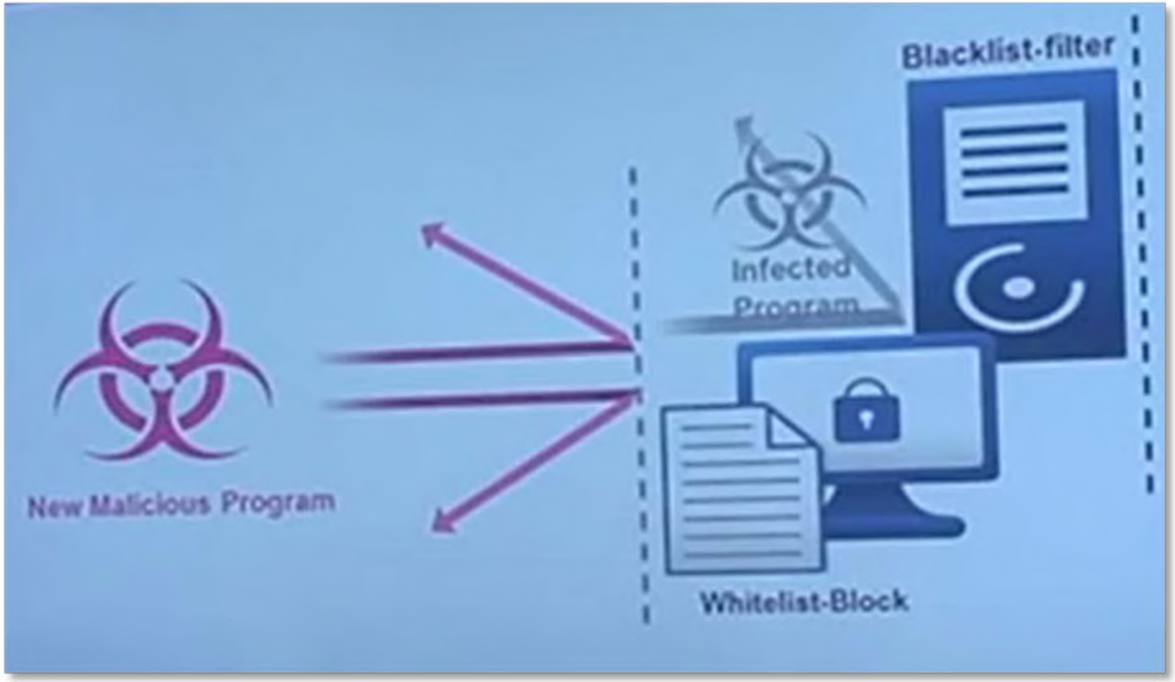
	Traditional Anti-Malware Solution	Harmonized whitelist technology Solution
Application control	Blacklist (known malicious applications)	Whitelist (authorized applications only)
Security Level	Low	High
Response	Reactive	Proactive defense
Environment	Internet-access environments	Closed network
Engine Size	Continually requires additional resources	Constant
Resource usage	High	Low
Maintenance	Frequent updates required	Minimal updating and patching

II. DI&C Solution

- Countermeasure for Cyber Security

- **Harmonization(compromise, negotiation,….) between safety and security is needed.**

=> *For applying ‘protection system(Anti-malware), combining whitelist and Blacklist technologies to meet the two contents.*



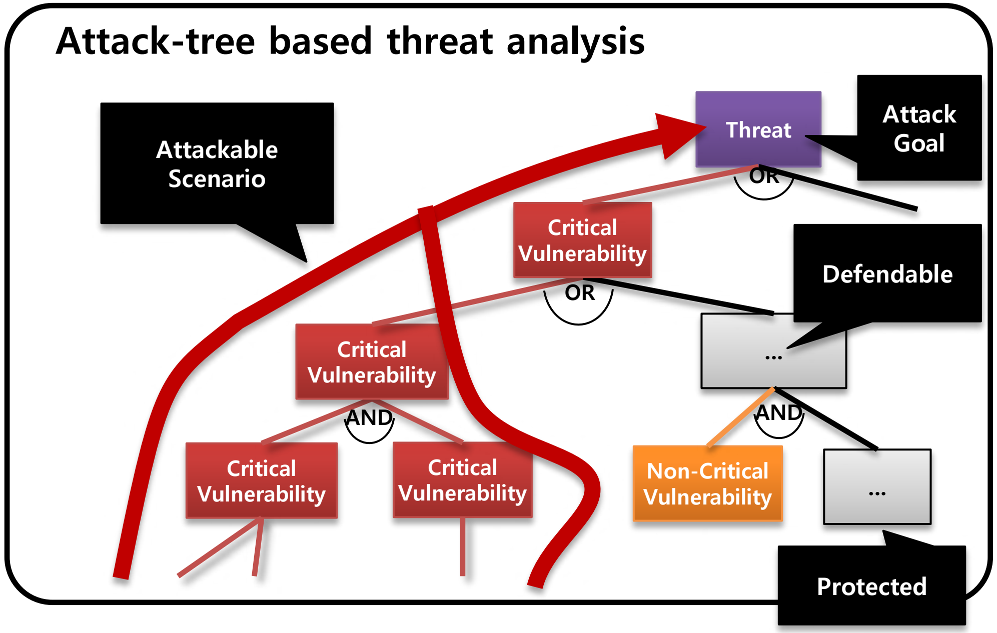
Multilayered Anti-malware Concept combining whitelist technologies

II. DI&C Solution

- Countermeasure for Cyber Security

Cyber Security - Elicitation of cybersecurity controls

- Categorize and prioritize vulnerabilities as critical and non-critical vulnerabilities



Critical vulnerability

- **Vulnerability directly involved in a threat**
- Nodes in an attackable path (scenario) of attack-tree
- **Elicit security controls**

Non-Critical vulnerability

- Vulnerability **not directly involved in a threat**
- Nodes in a non-attackable path (scenario)
- **Long-term improvement**

- **Threat-oriented elicitation of security controls**
  - **Focuses on critical vulnerability** directly related to a threat
- **APR-1400 with elicited cybersecurity controls**
  - Checked by white hackers (AhnLab) **through the penetrating test (more than 2,000 test cases), and failed to achieve attack goal**
  - Protected from the state-of-the-art (known and similar) attack techniques (e.g. STUXNET)

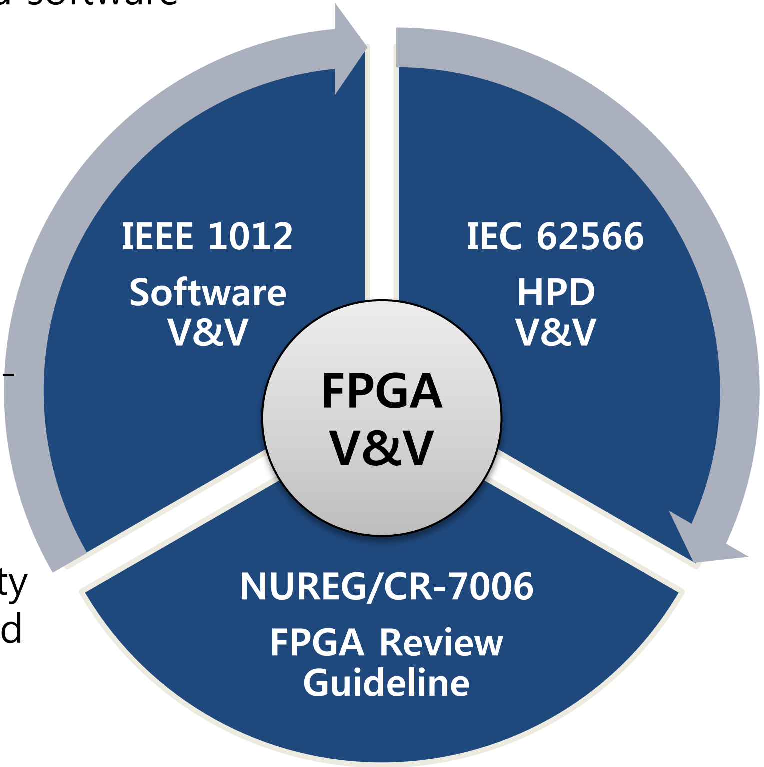
II. DI&C Solution

- Class 1E FPGA Platform – V&V

- **FPGA V&V is hard to be achieved with IEEE Std. 1012 (a basis for NPP software V&V)**
  - *[NUREG/CR-7006] IEEE-1002-2004 is a software-only standard, and it can not be directly applied to V&V process for FPGA-based systems. Even though the top level V&V processes and underlying activities are generic and can be used for FPGAs, the low level tasks are software specific, and not directly applicable to FPGAs.*
  - But, FPGA has mixed characteristics of hardware and software

➔ **Harmonized existing FGPA standards and technologies into IEEE Std. 1012-based SDLC (Software Development Life Cycle)**

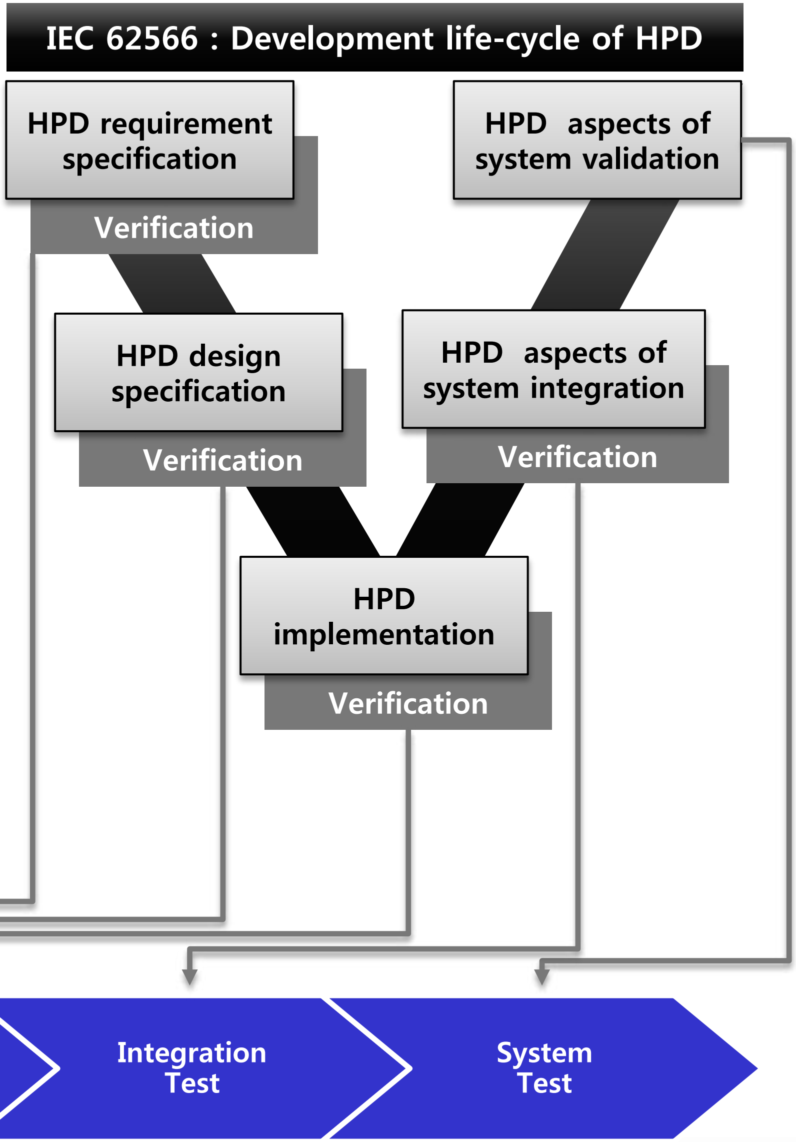
- **IEEE Std. 1012 :** Standard for Software Verification and Validation
- **NUREG/CR-7006 :** Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems
- **IEC 62566 :** Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions

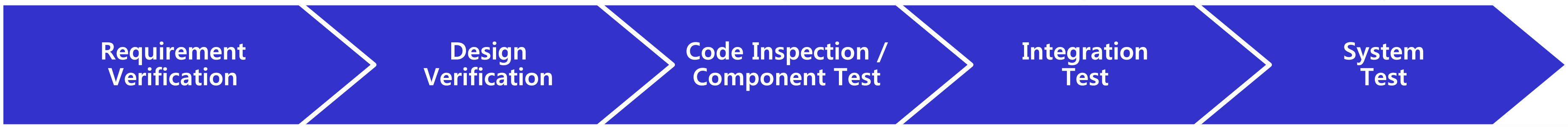


II. DI&C Solution

- Class 1E FPGA Platform – V&V

IEC 62566 Section 9 HPD Verification	Application Notes
9.1 General	▪ Independent V&V team
9.2 Verification plan	▪ Software V&V plan in the concept phase
9.3 Verification of the use of the pre-developed items	▪ Original software
9.4 Verification of the design and implementation	▪ SRS, SDD document evaluation
9.5 Test-benches	▪ Test-benches to fulfil requirement and path coverage
9.6 Test Coverage	▪ Path/Branch coverage for Component Test ▪ Requirement coverage for Integration Test
9.7 Test Execution	▪ Behavioral simulation using test benches ▪ Timing simulation
9.8 Static verification	▪ NUREG/CR-7006 based type and syntax checking


IEC 62566 : Development life-cycle of HPD
HPD requirement specification
Verification
HPD aspects of system validation
HPD design specification
Verification
HPD aspects of system integration
Verification
HPD implementation
Verification



Doosan Heavy Industries & Construction

※ *HPD : HDL-Programmed Device*

II. DI&C Solution

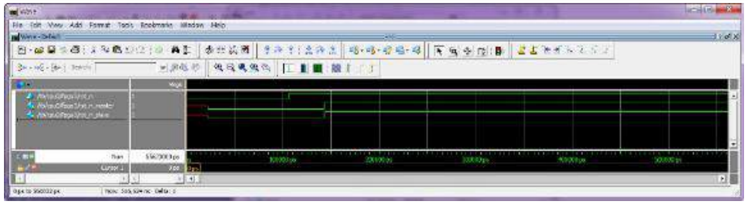
- Class 1E FPGA Platform – V&V

Requirement Verification → Design Verification → **Code Inspection / Component Test** → Integration (card, module) Test → System (FPGA controller) Test

- Behavior/timing simulation was performed on RTL/HDL code
- Test criteria : Path coverage, Requirement coverage
- Test environment : Host PC-based Simulation Environment

Host PC for Testing

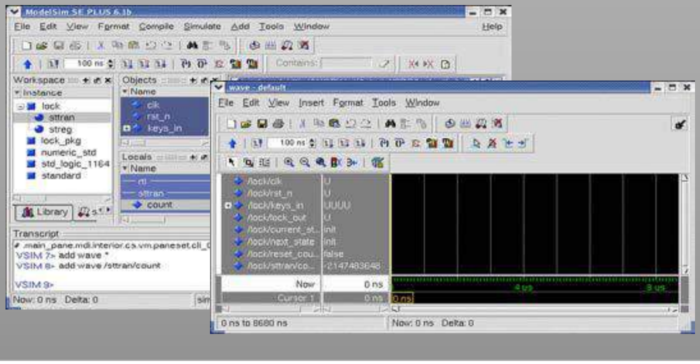
Test Case Simulation Result



STIMULI / Test Input → Target FPGA Under Test → RESPONSE / Test Result

Test Benches

Simulation Environment



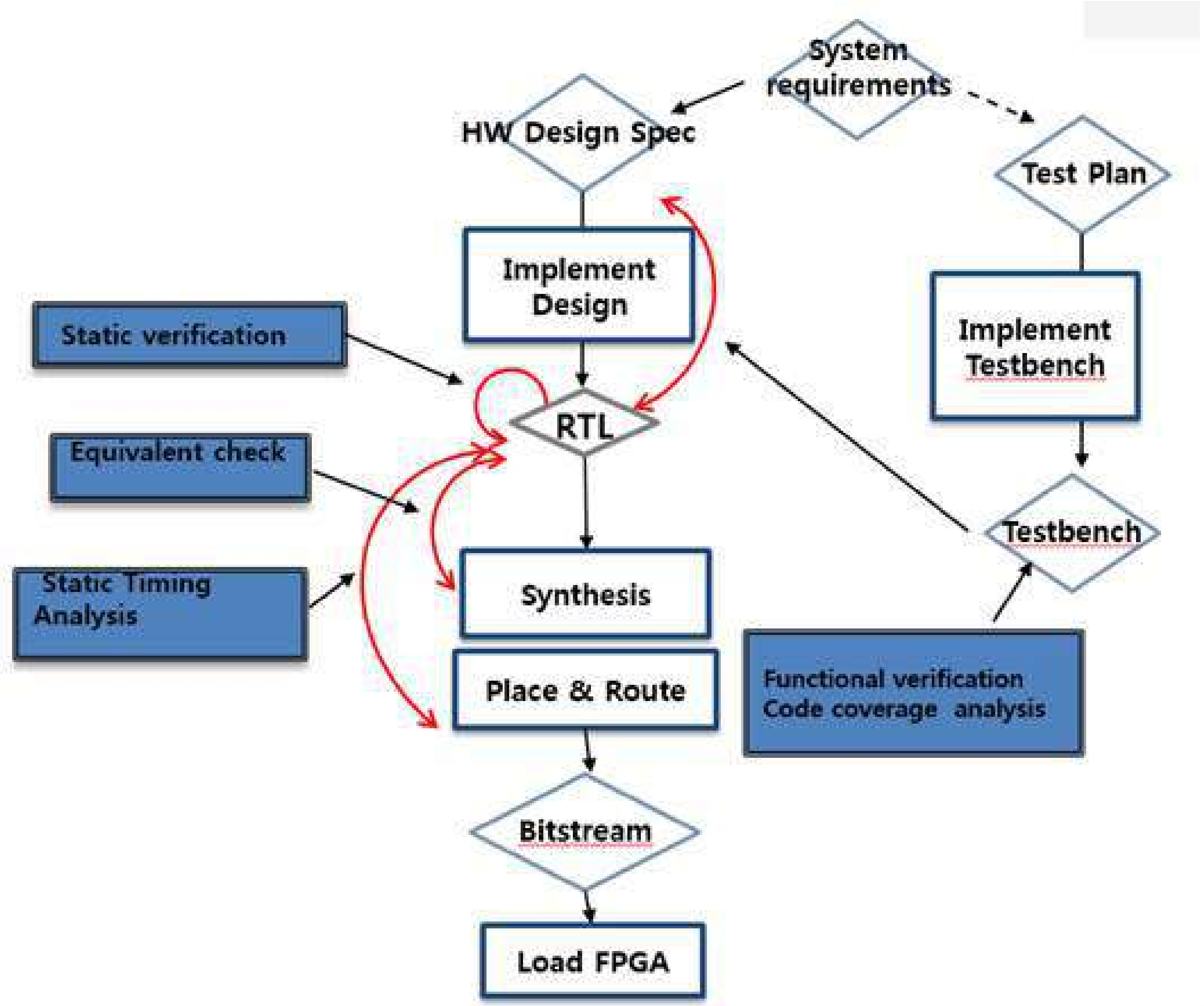
Transcript
```
# .main_pane.mdi.interior.cs.vm.paneset.cli_0
VSIM 7> add wave *
VSIM 8> add wave /sttran/count

VSIM 9>
```
Now: 0 ns Delta: 0

Host OS (Windows)

II. DI&C Solution

- Class 1E FPGA Platform – V&V



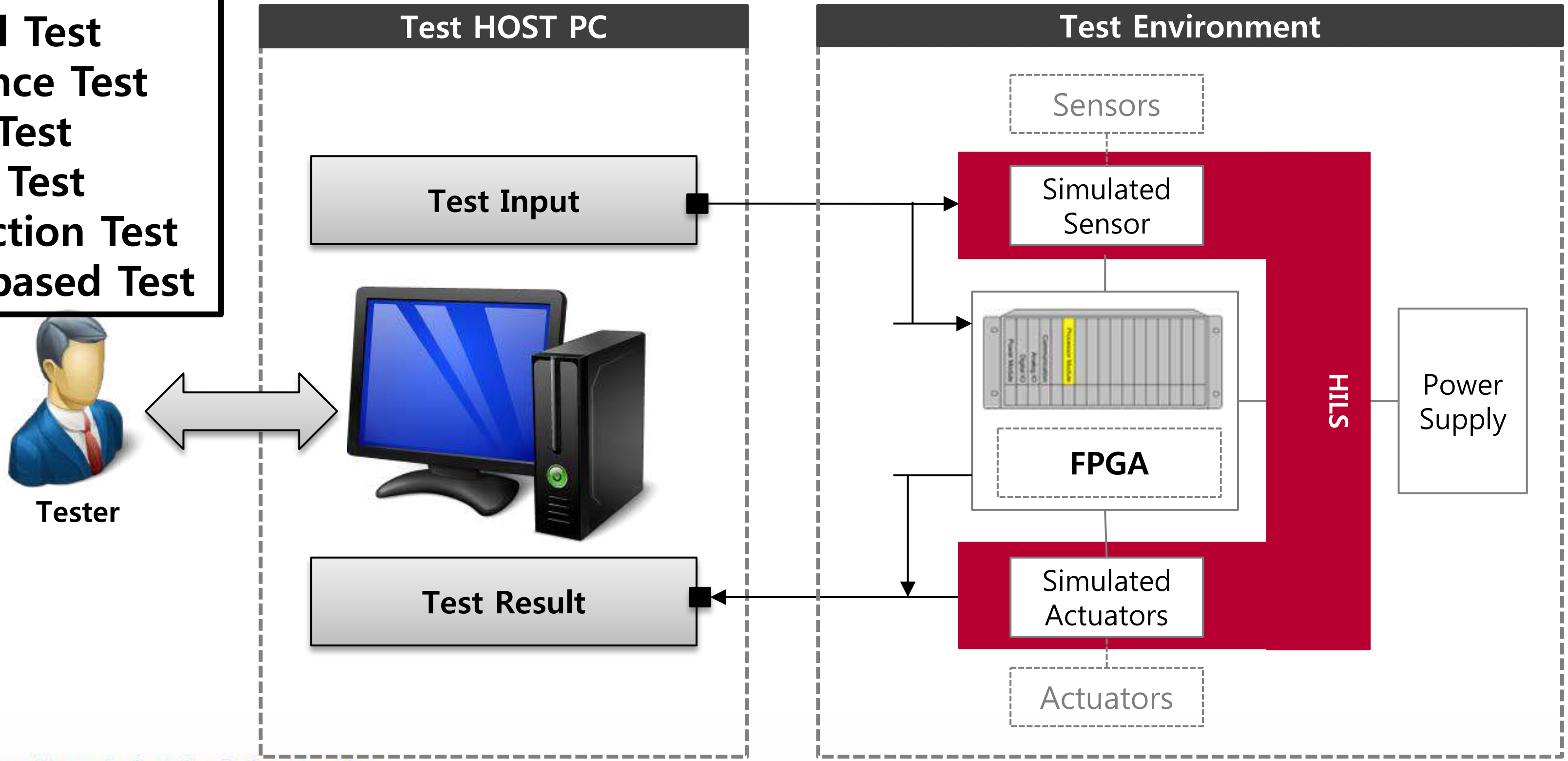
II. DI&C Solution

- Class 1E FPGA Platform – V&V

Requirement Verification → Design Verification → Code Inspection / Component Test → Integration (card, module) Test → **System (FPGA controller) Test**

- ➢ **Validated by Hardware-in-the-loop simulation**
- ➢ **Test criteria : Requirement coverage**
- ➢ **Test environment : Hardware-in-the-loop simulation environment**

➢ System Test
- **Functional Test**
- **Performance Test**
- **Interface Test**
- **Real-time Test**
- **Fault Injection Test**
- **Scenario based Test**

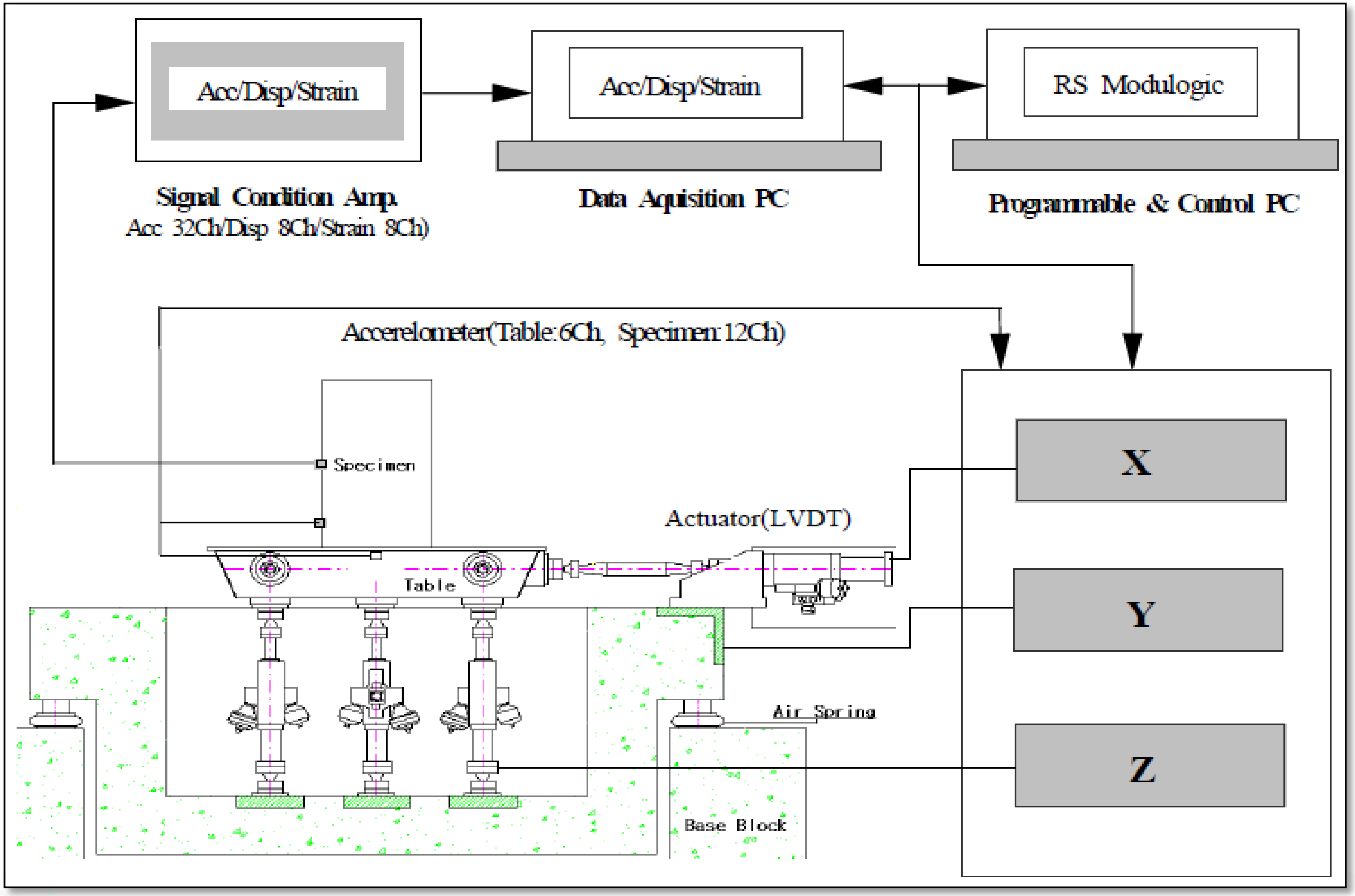


II. DI&C Solution

- Class 1E FPGA Platform – EQ

All EQ Testing Passed.

For example) Seismic (IEEE Std. 344 - 2004, Reg. Guide 1.29)

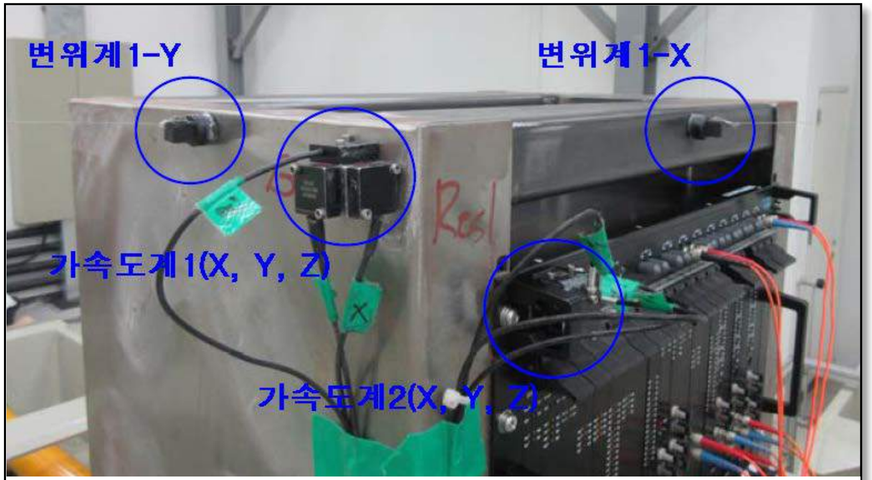


Seismic testing equipment Configuration

II. DI&C Solution

- Class 1E FPGA Platform – EQ

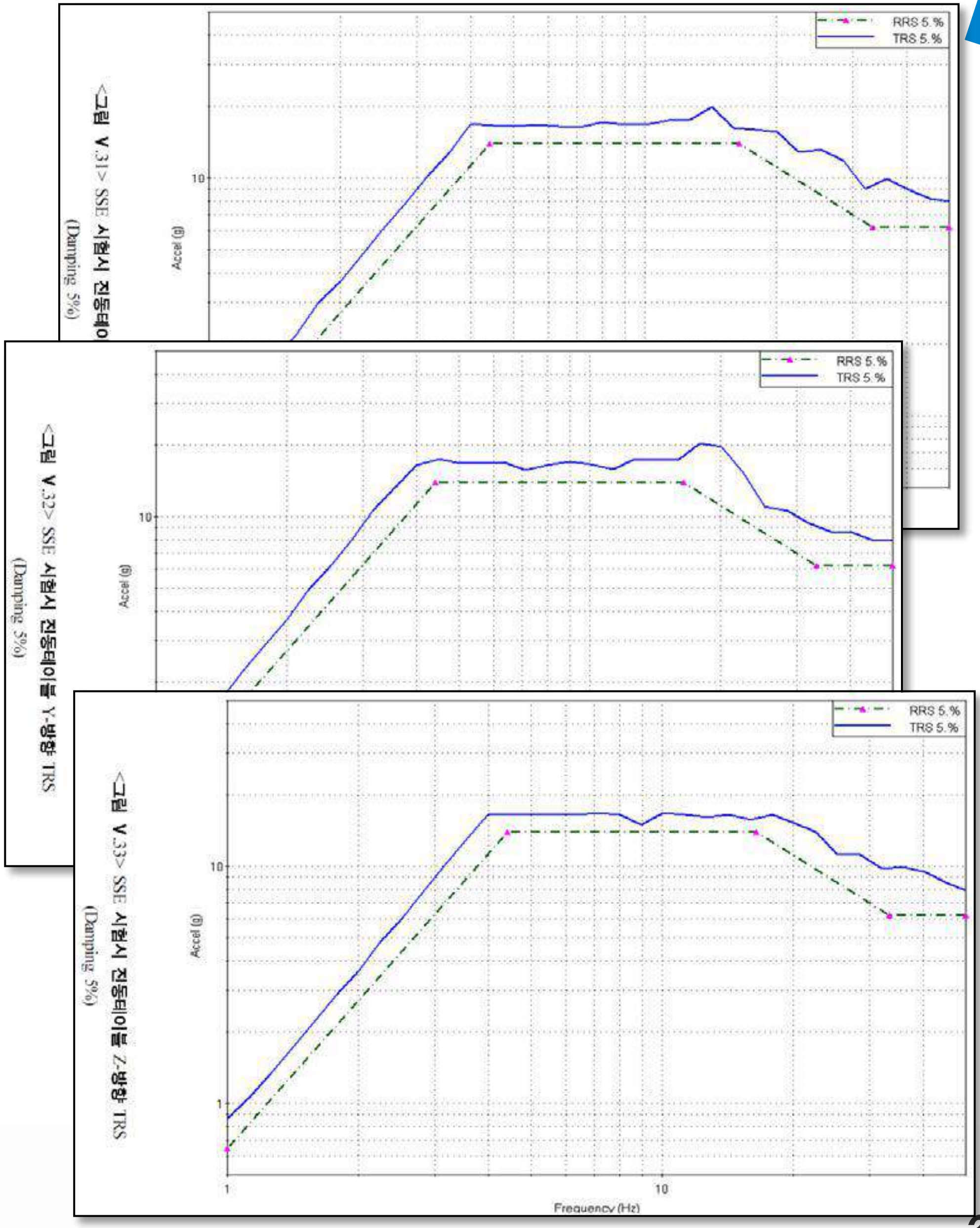
OBE 5 times & SSE 1 time (Demo)



Accelerometers and displacement meter installation location

Allowed during seismic testing standards

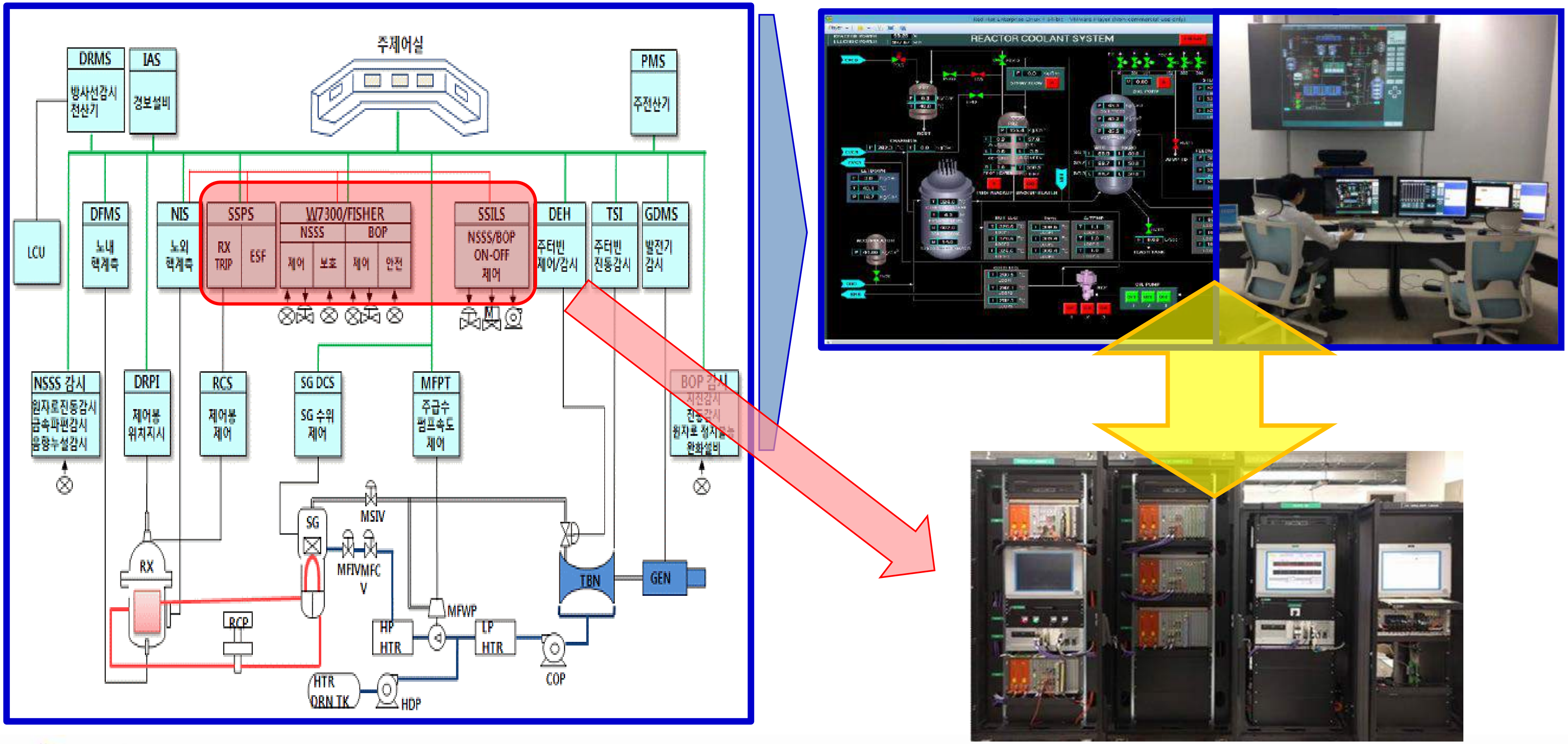
No	Signal type	Tolerance	Etc.
1	Analog Voltage	5 V ± 0.14%	4 Channel
2	Analog Current	12 mA ± 0.14%	1 channel
3	Digital Voltage	22 ~ 24 VDC	5 channel



III. Additional suggestions

- Code Simulator is good for validation of newly developed system

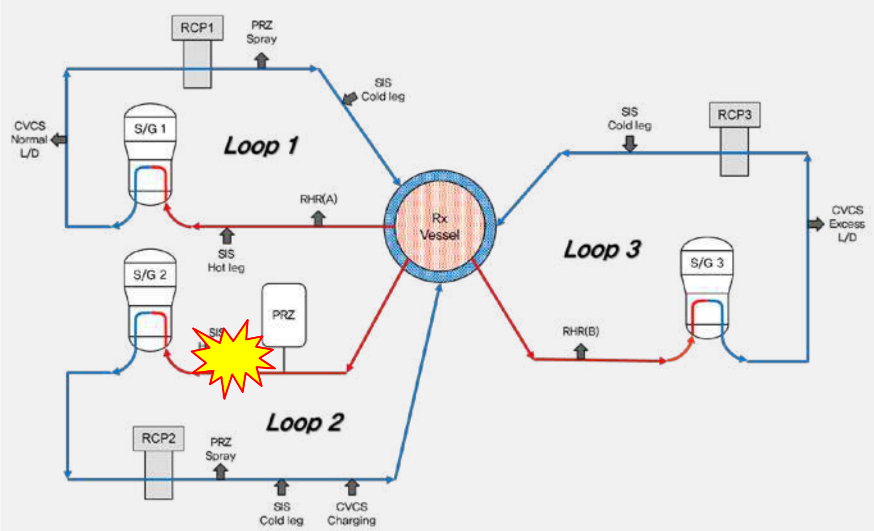
Hardware in the loop test facility including code simulator

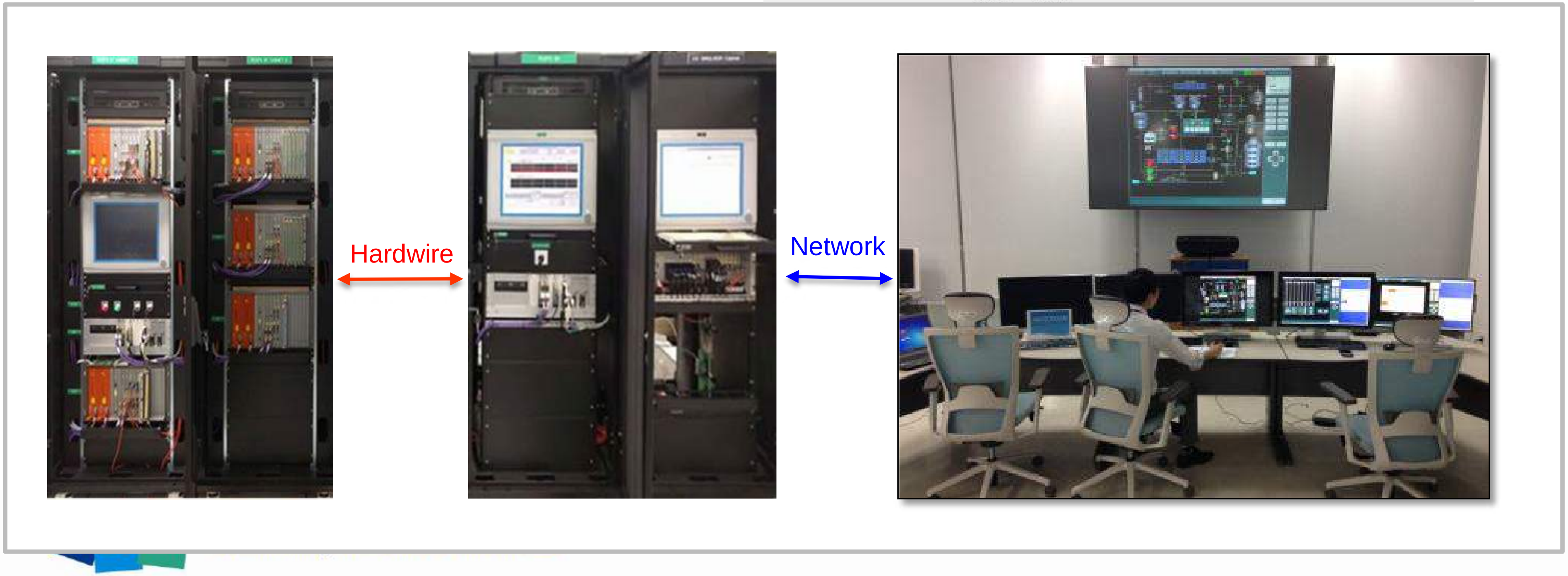


III. Additional suggestions

- Code Simulator is good for validation of newly developed system

Integrity confirm test using code simulator with malfunction scenario.





Thank you for listening

- ✓ Q&A by E-mail,
  to feel Lyon

chaeho.nam@doosan.com