



Doosan Heavy Industries & Construction

Design of Mutually Independent  
Controller Based Protection system  
considering CCF, SPV, and Full On-  
Line Surveillance Testing

Nam Chae Ho







Dallas, USA

Dec 4, 2017



**11<sup>th</sup> International Workshop on Application of FPGA in NPP**, in cooperation with **IAEA**  
hosted by **DOOSAN HFControls**, organized by **Sunport**, sponsored by **radiy** and **curtiss-wright**

# TABLE OF CONTENTS

-  I. Introduction
-  II. Existing Analog Protection System
-  III. Protection System with Diversity
-  IV. Test Results of Protection System using Code Simulator
-  V. Surveillance Test
-  VI. Conclusion

# I. Introduction

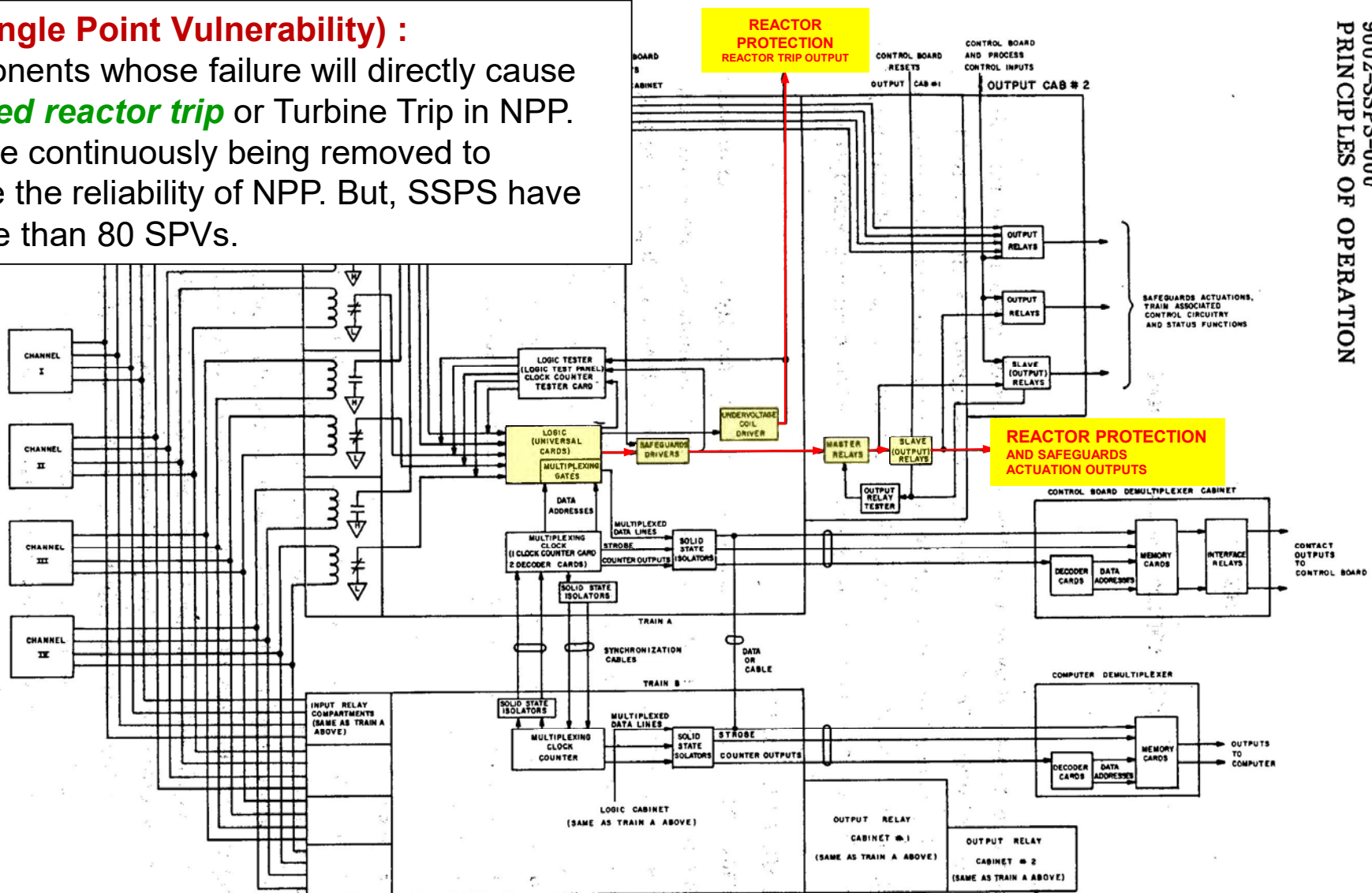
## - Background - SPV

### ■ SPV

#### SPV (Single Point Vulnerability) :

A components whose failure will directly cause **unwanted reactor trip** or Turbine Trip in NPP. SPVs are continuously being removed to enhance the reliability of NPP. But, SSPS have still more than 80 SPVs.

Figure 2-1. SSPS Block Diagram



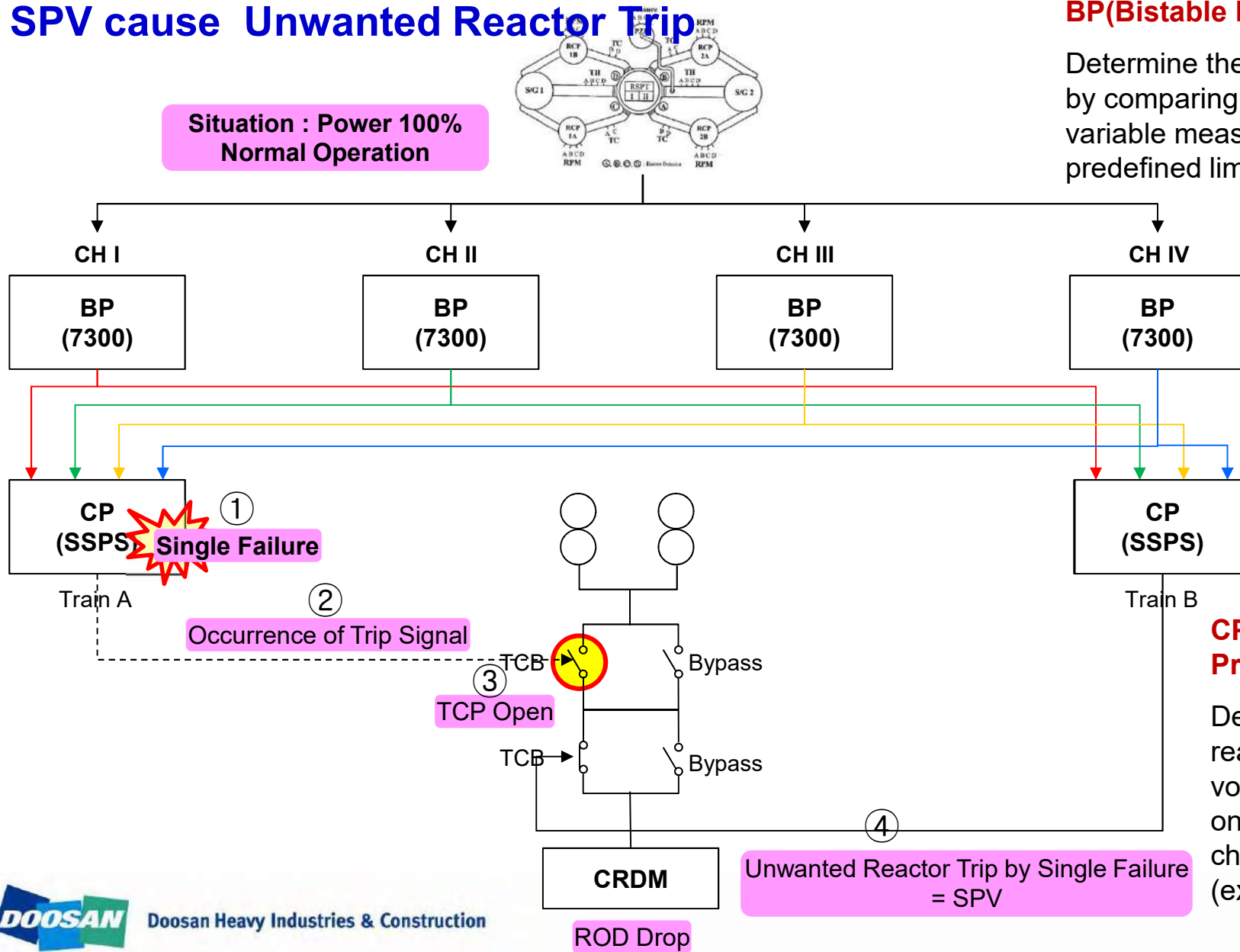
# I. Introduction

## - SPV example of the current Protection System

### ■ SPV cause Unwanted Reactor Trip

#### BP(Bistable Processor)

Determine the channel trip state by comparing the processor variable measurement with predefined limits



#### CP(Coincidence Processor)

Determine the reactor trip state by voting logic based on four pairs of channel trip inputs (ex : 2-out-of-4)

Unwanted Reactor Trip by Single Failure = SPV

# I. Introduction

## - Background - CCF

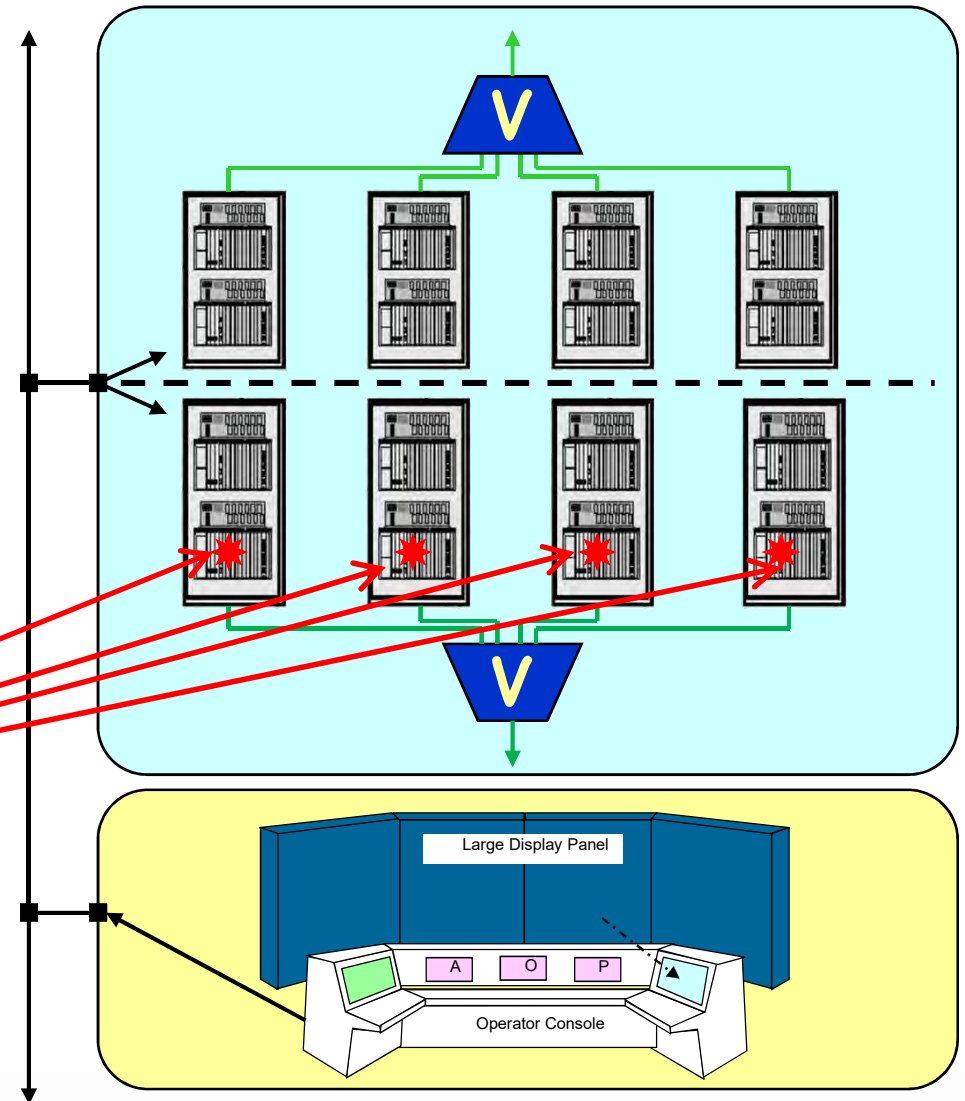
### ■ CCF

#### **CCF (Common Cause Failure) :**

Failure, that is the result of one or more events, causing **concurrent failures** of two or more separate **channels** in a multiple channel system, leading to system failure

#### **Identical (or similar) components**

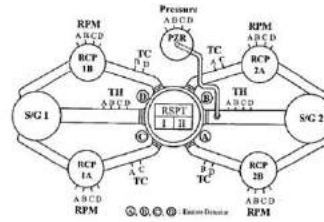
Same or causally related digital faults in multiple units and systems



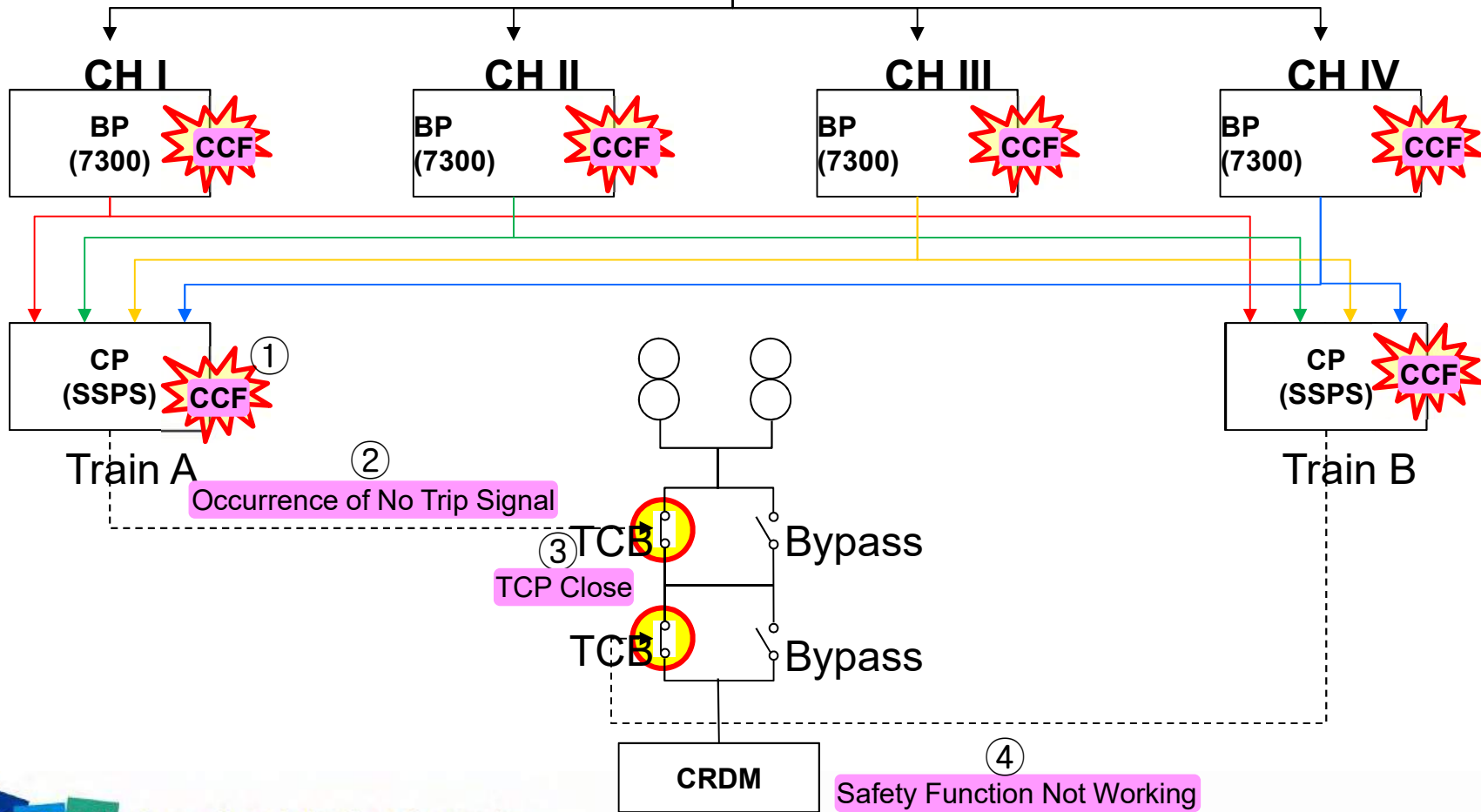
# I. Introduction

## - CCF example of the current Protection System

### ■ CCF cause ATWS



Situation : Abnormal Operation requiring Reactor Trip



# I. Introduction

## - Surveillance Test

### ■ Surveillance Test for Analog Protection System

1) 7300 Bistable Logic Test

2) SSPS Input Relay Test

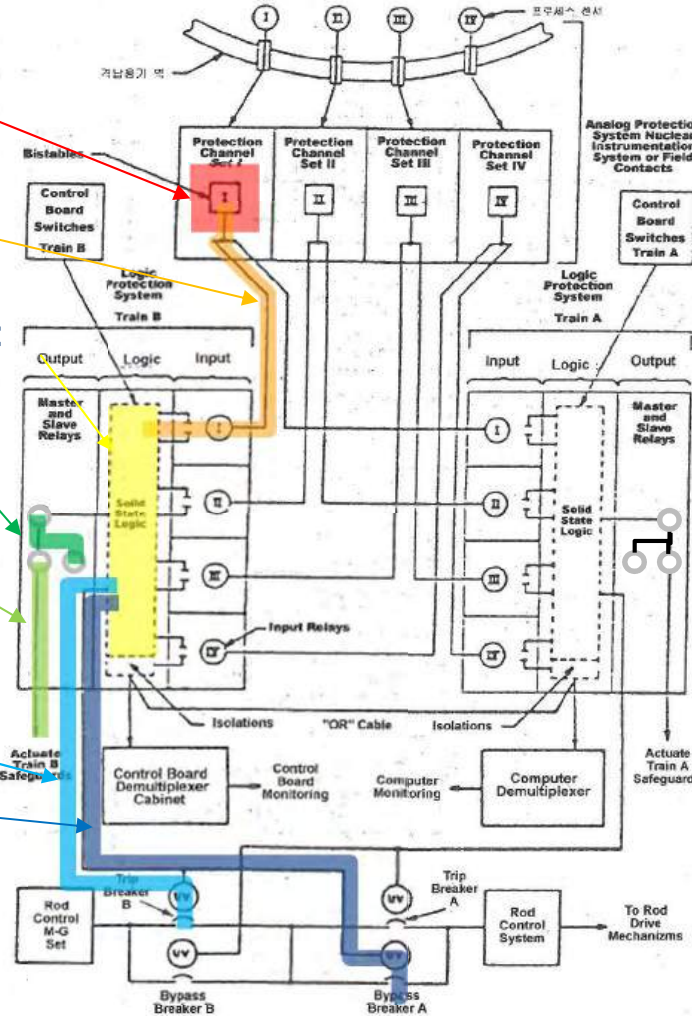
3) SSPS Coincidence Logic Test (semiautomatic test panel)

4) Master/Slave Relay Test

5) ESFAS Signal Test (Safeguard Test Cabinet)

6) RTB Test

7) Bypass Test



**Difficult**

✓ It should be split into several tests for full test coverage

**Limited**

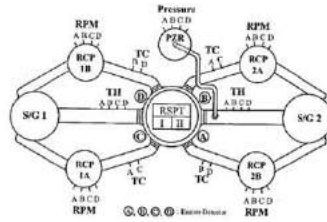
✓ It is impossible to test entire Protection System in

**Time-consuming**

✓ Test of Analog Protection System is complicated and needs much time

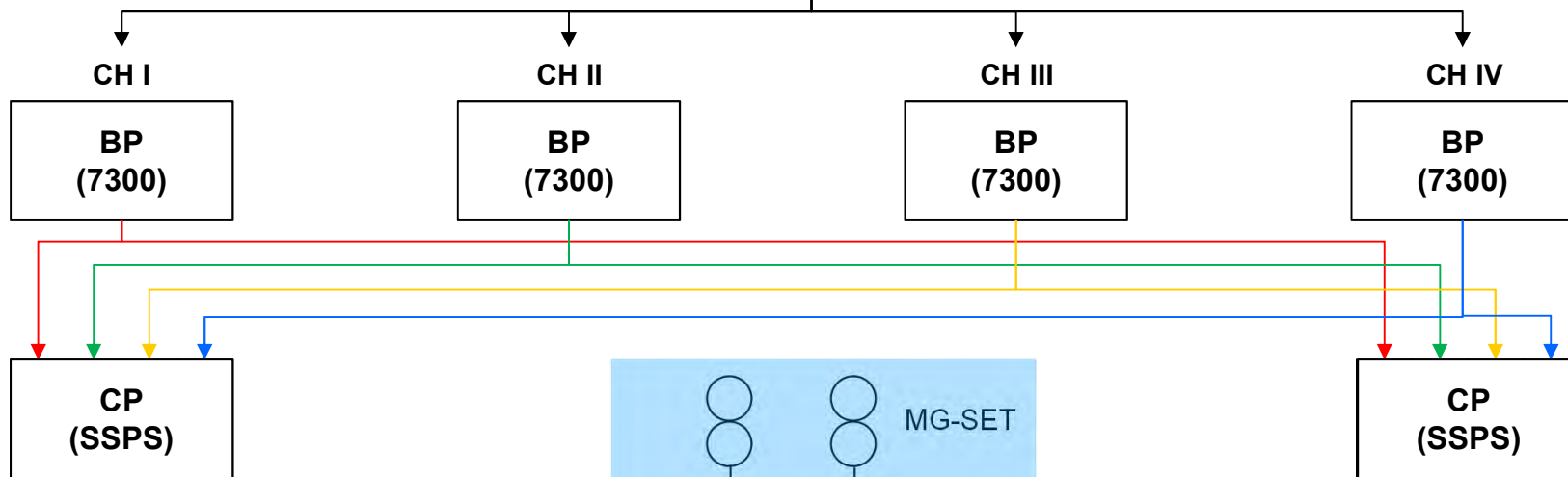
# II. Existing Analog Protection System

- Vulnerable to SPV and Testability



## BP(Bistable Processor)

Determine the channel trip state by comparing the processor variable measurement with predefined limits



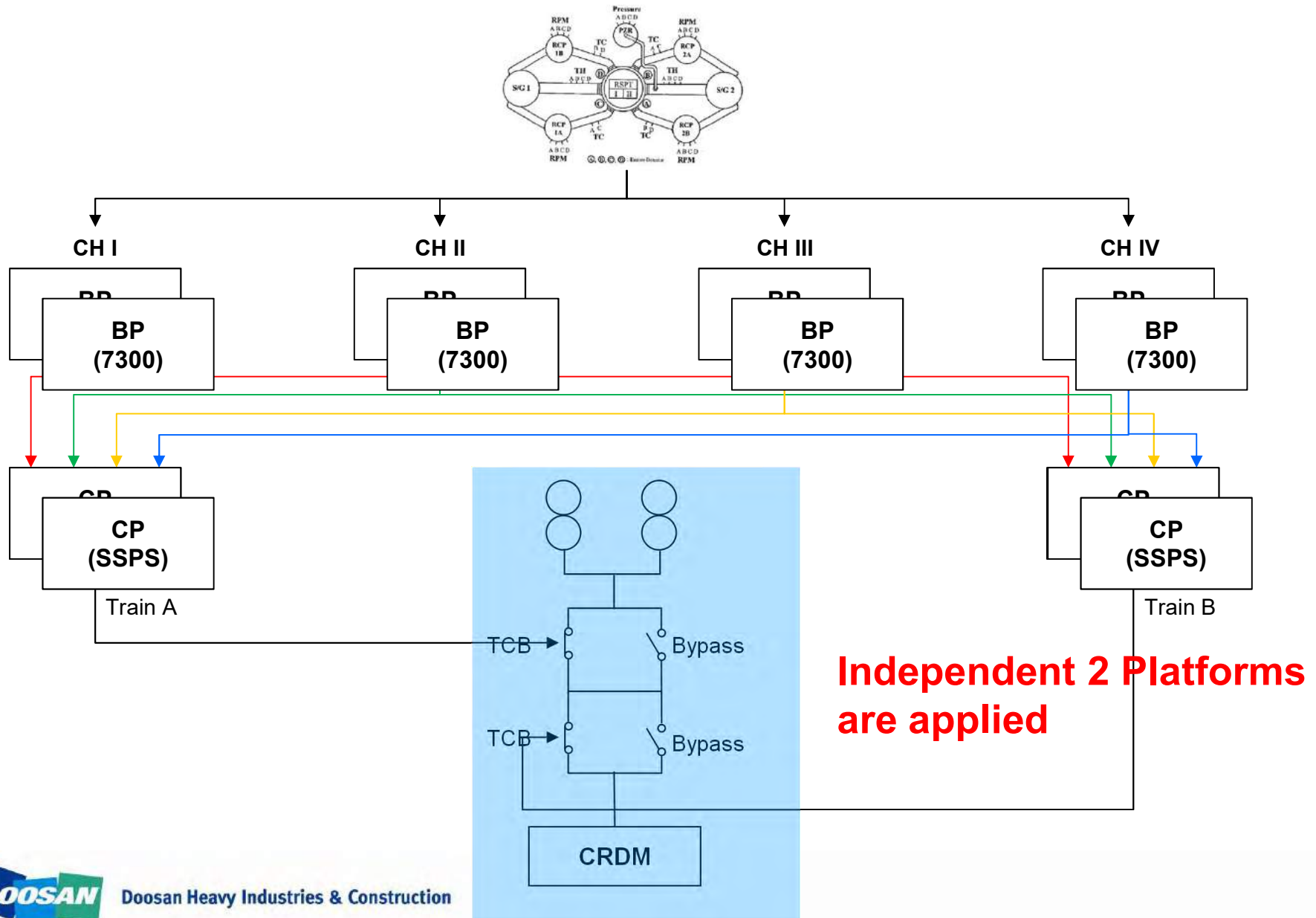
## CP(Coincidence Processor)

Determine the reactor trip state by voting logic based on four pairs of channel trip inputs (ex : 2-out-of-4)



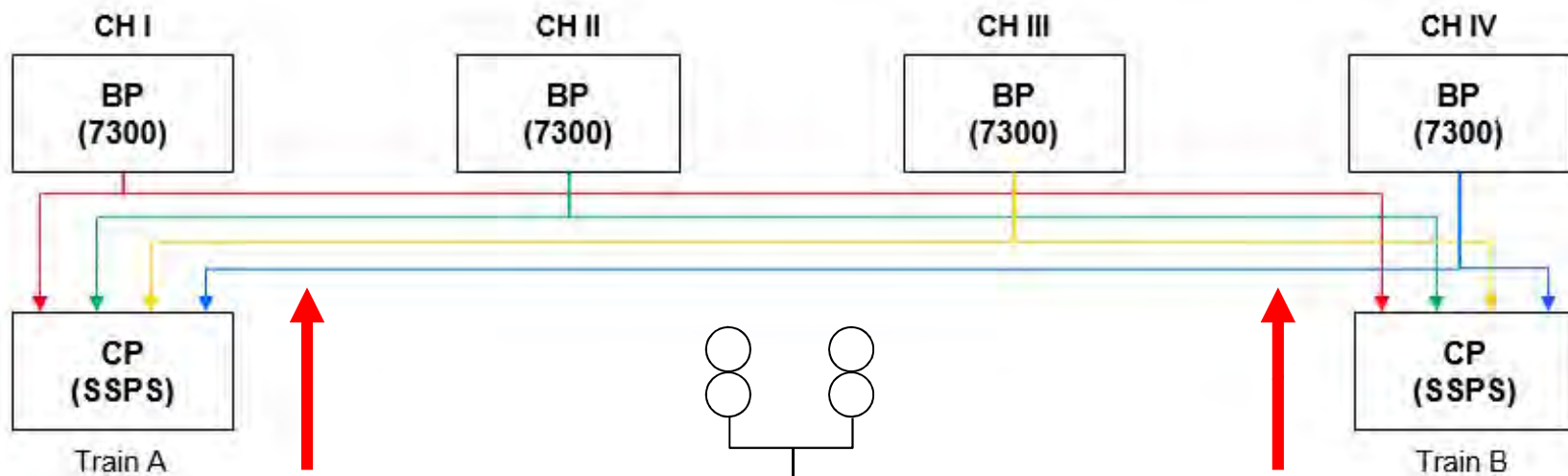
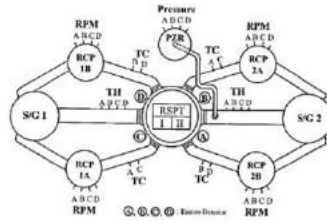
# III. Protection System with Diversity

## - Countermeasure for SPV and CCF



# III. Protection System with Diversity

- Countermeasure for SPV and CCF



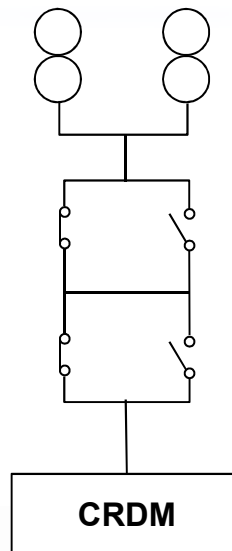
**FLC based  
Protection System**

**PLC based  
Protection System**



**Doosan FPGA**

Doosan Heavy Industries & Construction



**CRDM**



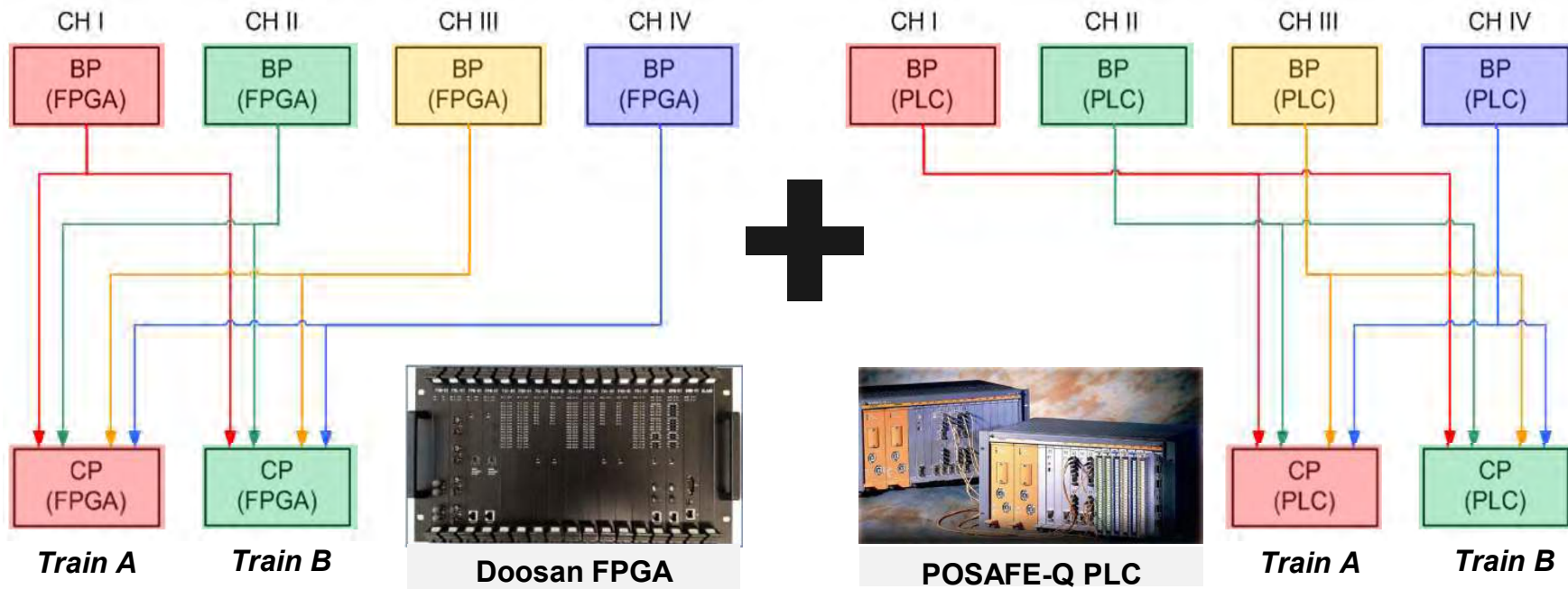
**POSAFE-Q PLC**

# III. Protection System with Diversity

## - Countermeasure for CCF Issues

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

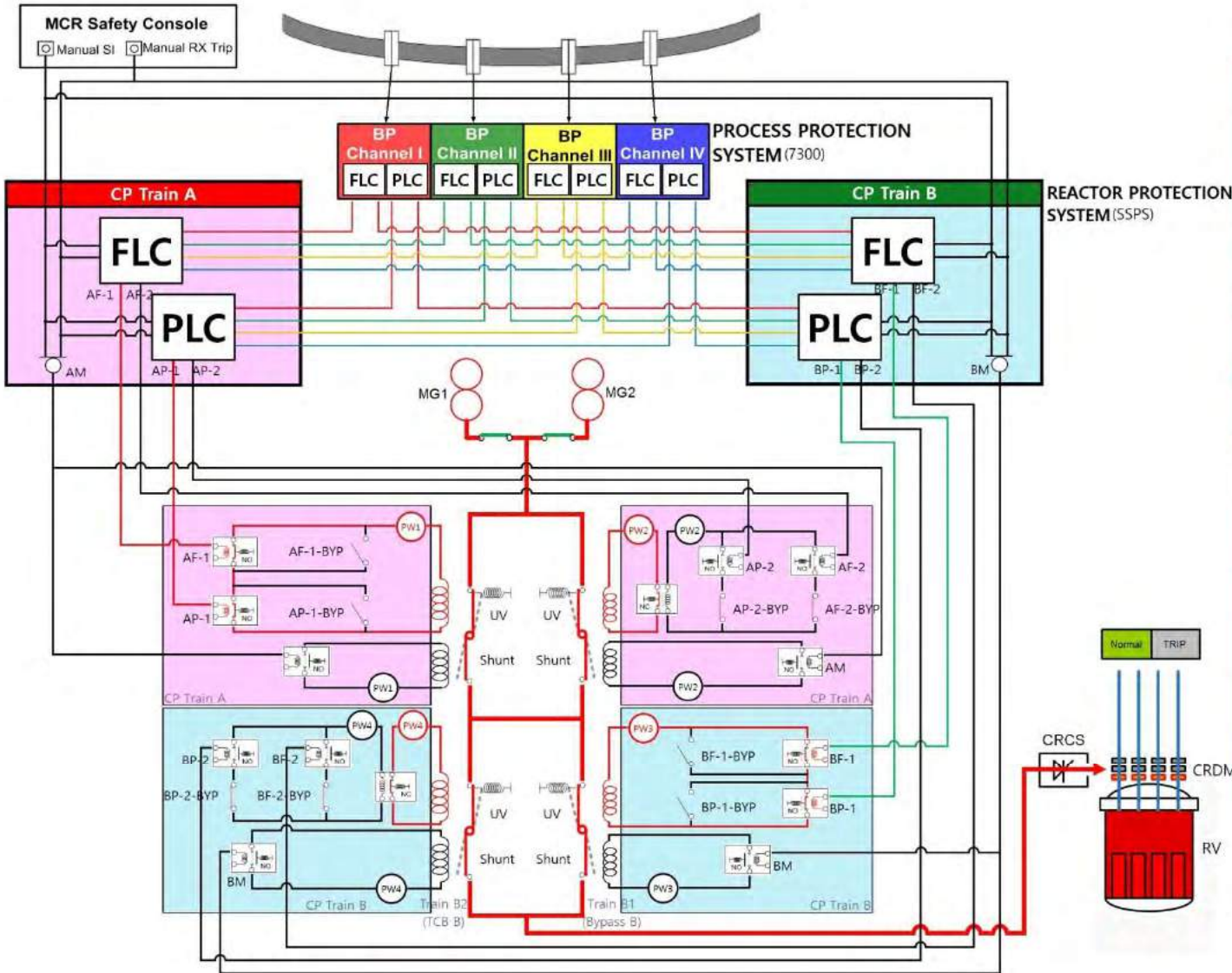
- ✓ *As is – Class 1E Protection System and Non-Class 1E DPS*
- ✓ *To be – Class 1E independent Protection System using different platform*
- ✓ *Independent protection scheme designs using different controller platforms can mitigate ATWS by CCF*



# III. Protection System with Diversity

## - Countermeasure for CCF Issues

■ Different Platform of PPS will resolve the CCF Issues (Rx Power 100%)



ALARM		ESFAS	
OT ΔT RCT TRIP	PRZ HI PRESS RCT TRIP	PWR RANGE HI FLUX RATE RCT TRIP	SIS
OP ΔT RCT TRIP	PRZ LO PRESS & P-7 RCT TRIP	RCS FLOW LO AT HI PWR RCT TRIP	CIS-A
CTMT PRESS HI SI RCT TRIP	SOURCE RANGE HI FLUX RCT TRIP	RCS FLOW LO AT LO PWR RCT TRIP	CIS-B
MANUAL RCT TRIP	INTMD RANGE HI FLUX RCT TRIP	SG 1.2.3 WTR LEVEL LO-LO RCT TRIP	CSS
MANUAL SI RCT TRIP	PWR RANGE HI FLUX HI SETPT RCT TRIP	TBN TRIP & P-7 RCT TRIP	FWIS
PRZ HI LEVEL RCT TRIP	PWR RANGE HI FLUX LO SETPT RCT TRIP	MSL PRESS LOW SI RCT TRIP	MSIS

CONTROL		PERMISSIVE	
C-1 High Neutron Flux Rod Stop Interlock	C-7 Loss of Load Interlock	P-4 Reactor Trip Permissive	P-11 Low Pressurizer Pressure SI Block Permissive
C-2 Overpower Rod Stop Interlock	C-8 Turbine Tripped Interlock	P-6 Source Range Block Permissive	P-12 High Steam Flow SI Block Permissive
C-3 OT ΔT Rod Stop and Turbine Runback Interlock	C-9 Condenser Available Interlock	P-7 At-Power Permissive	P-13 Turbine At-Power Permissive
C-4 OP ΔT Rod Stop and Turbine Runback Interlock	C-11 Control Bank D Rod Withdrawal Limit Interlock	P-8 Three Loop Flow Permissive	P-14 Steam Generator High Level Override
C-5 Low Power Interlock	C-16 Turbine Stop Loading Interlock	P-10 Nuclear At-Power Permissive	

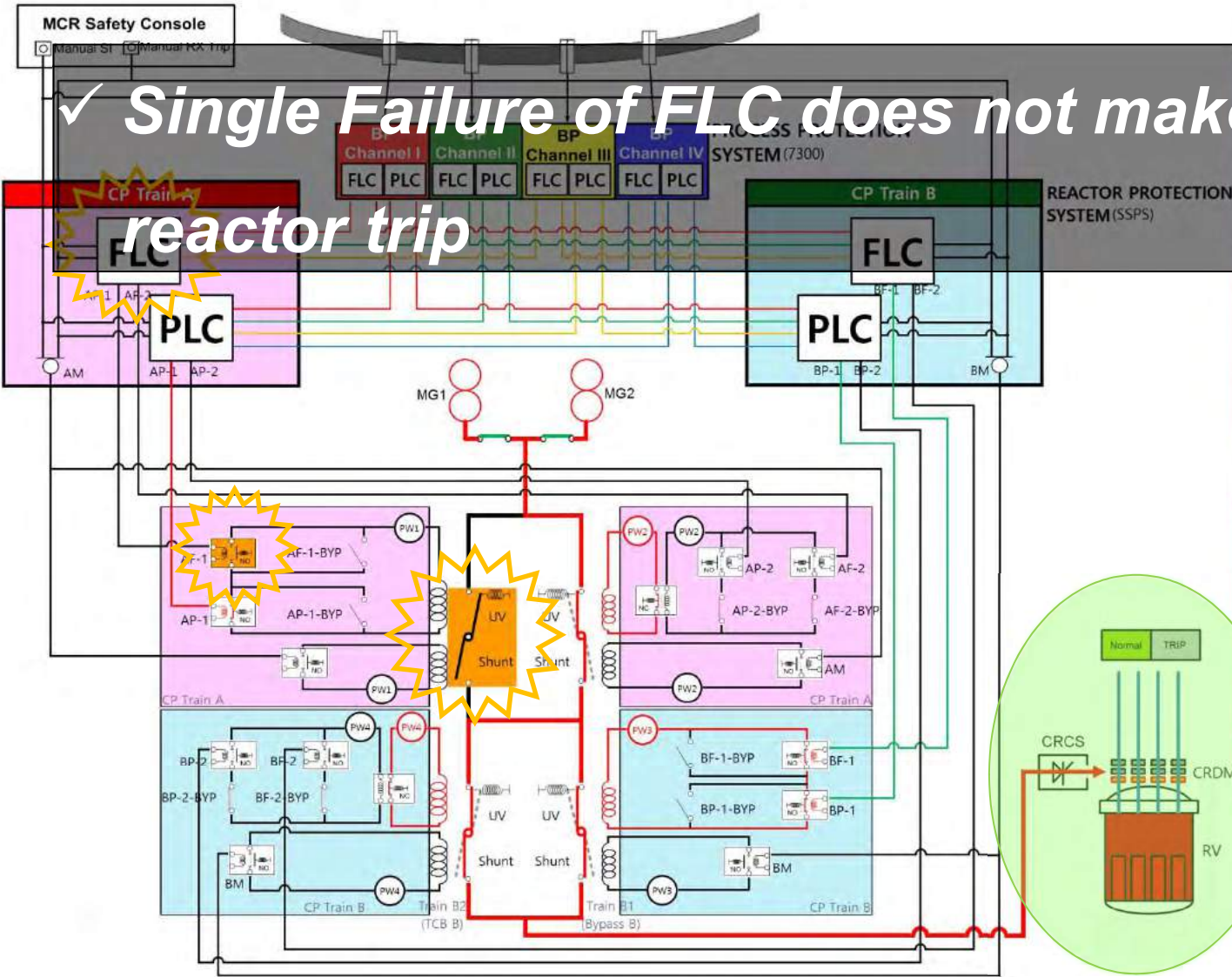
No photography of this exhibition  
Due to conservation and copyright restrictions.

Designed by DOOSAN Nuclear I&C Since 2016/11/3  
Patent No KR10-2016-0145468, US15/646611, CN201710532503.7,  
PH11-2017-000342 and BR10-2017-026123-9

# IV. Test Results of Protection System using Code Simulator

## - Countermeasure for CCF Issues

### ■ Case Study #1 SPV of FLC based Protection System



ALARM			ESFAS
OT ΔT RCT TRIP	PRZ HI PRESS RCT TRIP	PWR RANGE HI FLUX RCT TRIP	SIS
OP ΔT RCT TRIP	PRZ LO PRESS & P-7 RCT TRIP	RCS FLOW LO AT HI PWR RCT TRIP	CIS-A
CTMT PRESS HI SI RCT TRIP	SOURCE RANGE HI FLUX RCT TRIP	RCS FLOW LO AT LO PWR RCT TRIP	CIS-B
MANUAL RCT TRIP	INTMD RANGE HI FLUX RCT TRIP	SG 1,2,3 WTR LEVEL LO-LO RCT TRIP	CSS
MANUAL SI RCT TRIP	PWR RANGE HI FLUX HI SETPT RCT TRIP	TBN TRIP & P-7 RCT TRIP	FWIS
PRZ HI LEVEL RCT TRIP	PWR RANGE HI FLUX LO SETPT RCT TRIP	MSL PRESS LOW SI RCT TRIP	MSIS

CONTROL		PERMISSIVE	
C-1 High Neutron Flux Rod Stop Interlock	C-7 Loss of Load Interlock	P-4 Reactor Trip Permissive	P-11 Low Pressurizer Pressure SI Block Permissive
C-2 Overpower Rod Stop Interlock	C-8 Turbine Tripped Interlock	P-6 Source Range Block Permissive	P-12 High Steam Flow SI Block Permissive
C-3 OT ΔT Rod Stop and Turbine Runback Interlock	C-9 Condenser Available Interlock	P-7 At-Power Permissive	P-13 Turbine At-Power Permissive
C-4 OP ΔT Rod Stop and Turbine Runback Interlock	C-11 Control Bank D Rod Withdrawal Limit Interlock	P-8 Three Loop Flow Permissive	P-14 Steam Generator High Level Override
C-5 Low Power Interlock	C-16 Turbine Stop Loading Interlock	P-10 Nuclear At-Power Permissive	

No photography of this exhibition  
Due to conservation and copyright restrictions.

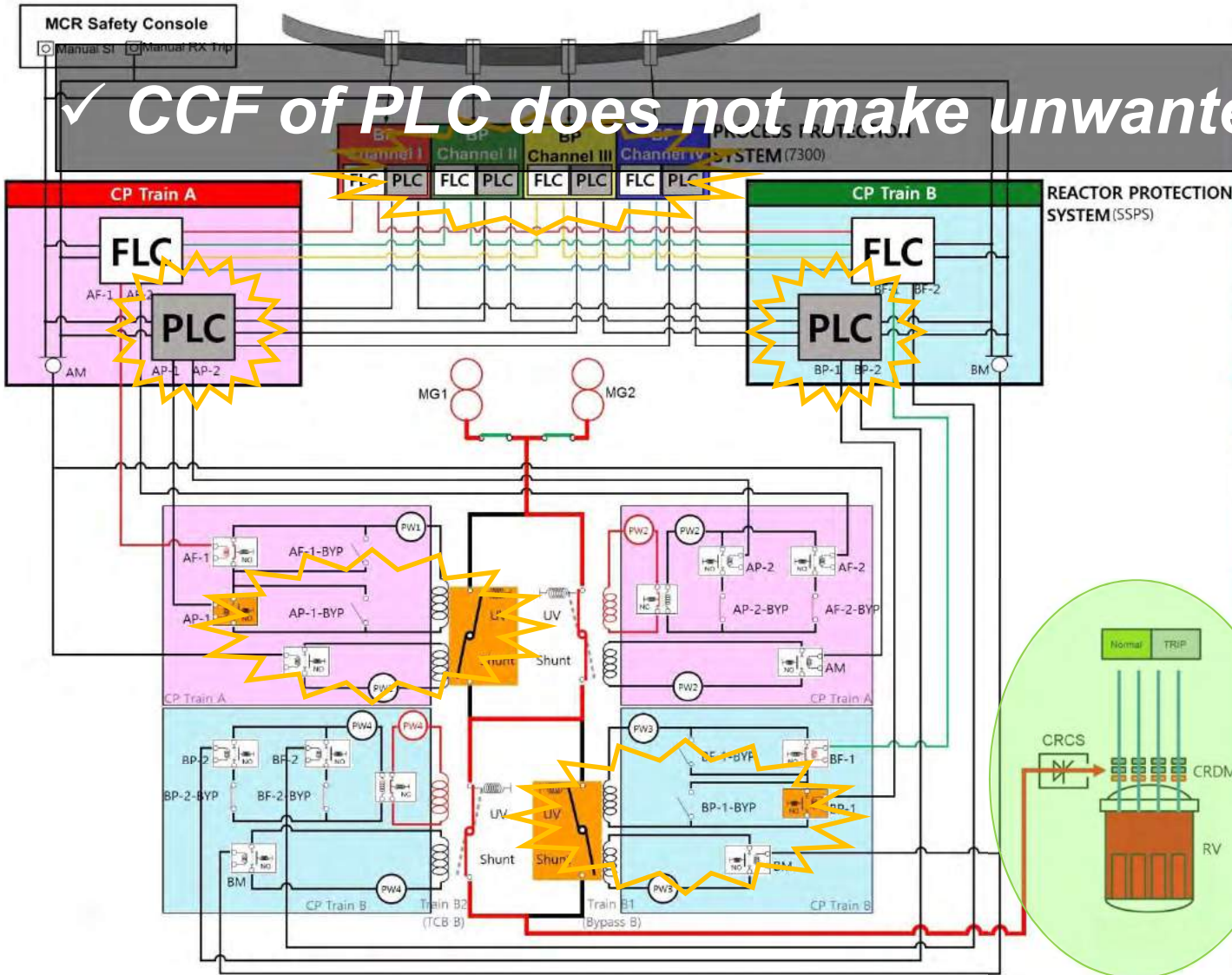
Designed by DOOSAN Nuclear I&C Since 2016/11/3  
Patent No KR10-2016-0145468, US15/646611, CN201710532503.7,  
PH11-2017-000342 and BR10-2017-026123-9

# IV. Test Results of Protection system using Code Simulator

## - Countermeasure for CCF Issues

### ■ Case Study #2 CCF of PLC based Protection System

✓ CCF of PLC does not make unwanted reactor trip



ALARM			ESFAS
OT ΔT RCT TRIP	PRZ HI PRESS RCT TRIP	PWR RANGE HI FLUX RATE	SIS
OP ΔT RCT TRIP	PRZ LO PRESS & P-7 RCT TRIP	RCS FLOW LO AT HI PWR RCT TRIP	CIS-A
CTMT PRESS HI SI RCT TRIP	SOURCE RANGE HI FLUX RCT TRIP	RCS FLOW LO AT LO PWR RCT TRIP	CIS-B
MANUAL RCT TRIP	INTMD RANGE HI FLUX RCT TRIP	SG 1.2.3 WTR LEVEL LO-LO RCT TRIP	CSS
MANUAL SI RCT TRIP	PWR RANGE HI FLUX HI SETPT RCT TRIP	TBN TRIP & P-7 RCT TRIP	FWIS
PRZ HI LEVEL RCT TRIP	PWR RANGE HI FLUX LO SETPT RCT TRIP	MSL PRESS LOW SI RCT TRIP	MSIS

CONTROL		PERMISSIVE	
C-1 High Neutron Flux Rod Stop Interlock	C-7 Loss of Load Interlock	P-4 Reactor Trip Permissive	P-11 Low Pressurizer Pressure SI Block Permissive
C-2 Overpower Rod Stop Interlock	C-8 Turbine Tripped Interlock	P-6 Source Range Block Permissive	P-12 High Steam Flow SI Block Permissive
C-3 OT ΔT Rod Stop and Turbine Runback Interlock	C-9 Condenser Available Interlock	P-7 At-Power Permissive	P-13 Turbine At-Power Permissive
C-4 OP ΔT Rod Stop and Turbine Runback Interlock	C-11 Control Bank D Rod Withdrawal Limit Interlock	P-8 Three Loop Flow Permissive	P-14 Steam Generator High Level Override
C-5 Low Power Interlock	C-16 Turbine Stop Loading Interlock	P-10 Nuclear At-Power Permissive	

No photography of this exhibition  
Due to conservation and copyright restrictions.

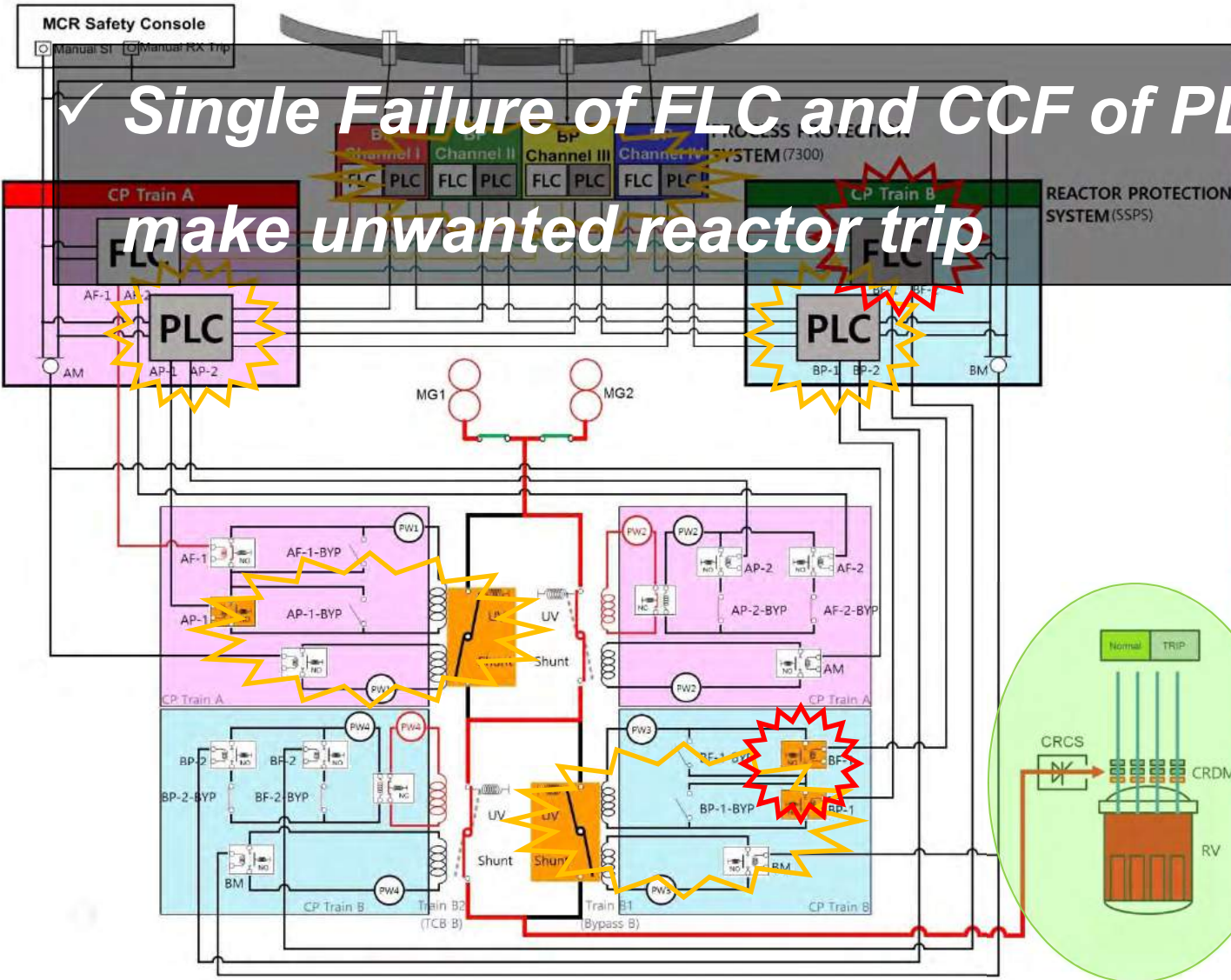
Designed by DOOSAN Nuclear I&C Since 2016/11/3  
Patent No KR10-2016-0145468, US15/646611, CN201710532503.7,  
PH11-2017-000342 and BR10-2017-026123-9

# IV. Test Results of Protection system using Code Simulator

## - Countermeasure for CCF Issues

### ■ Case Study #3 Combined PLC CCF & FLC SPV at Protection System

✓ *Single Failure of FLC and CCF of PLC does not make unwanted reactor trip*



ALARM			ESFAS
OP ΔT RCT TRIP	PRZ HI PRESS RCT TRIP	PWR RANGE HI FLUX RCT TRIP	SIS
OP ΔT RCT TRIP	PRZ LO PRESS & P-7 RCT TRIP	RCS FLOW LO AT HI PWR RCT TRIP	CIS-A
CTMT PRESS HI SI RCT TRIP	SOURCE RANGE HI FLUX RCT TRIP	RCS FLOW LO AT LO PWR RCT TRIP	CIS-B
MANUAL RCT TRIP	INTMD RANGE HI FLUX RCT TRIP	SG 1,2,3 WTR LEVEL LO-LO RCT TRIP	CSS
MANUAL SI RCT TRIP	PWR RANGE HI FLUX HI SETPT RCT TRIP	TBN TRIP & P-7 RCT TRIP	FWIS
PRZ HI LEVEL RCT TRIP	PWR RANGE HI FLUX LO SETPT RCT TRIP	MSL PRESS LOW SI RCT TRIP	MSIS

CONTROL		PERMISSIVE	
C-1 High Neutron Flux Rod Stop Interlock	C-7 Loss of Load Interlock	P-4 Reactor Trip Permissive	P-11 Low Pressurizer Pressure SI Block Permissive
C-2 Overpower Rod Stop Interlock	C-8 Turbine Tripped Interlock	P-6 Source Range Block Permissive	P-12 High Steam Flow SI Block Permissive
C-3 OP ΔT Rod Stop and Turbine Runback Interlock	C-9 Condenser Available Interlock	P-7 At-Power Permissive	P-13 Turbine At-Power Permissive
C-4 OP ΔT Rod Stop and Turbine Runback Interlock	C-11 Control Bank D Rod Withdrawal Limit Interlock	P-8 Three Loop Flow Permissive	P-14 Steam Generator High Level Override
C-5 Low Power Interlock	C-16 Turbine Stop Loading Interlock	P-10 Nuclear At-Power Permissive	

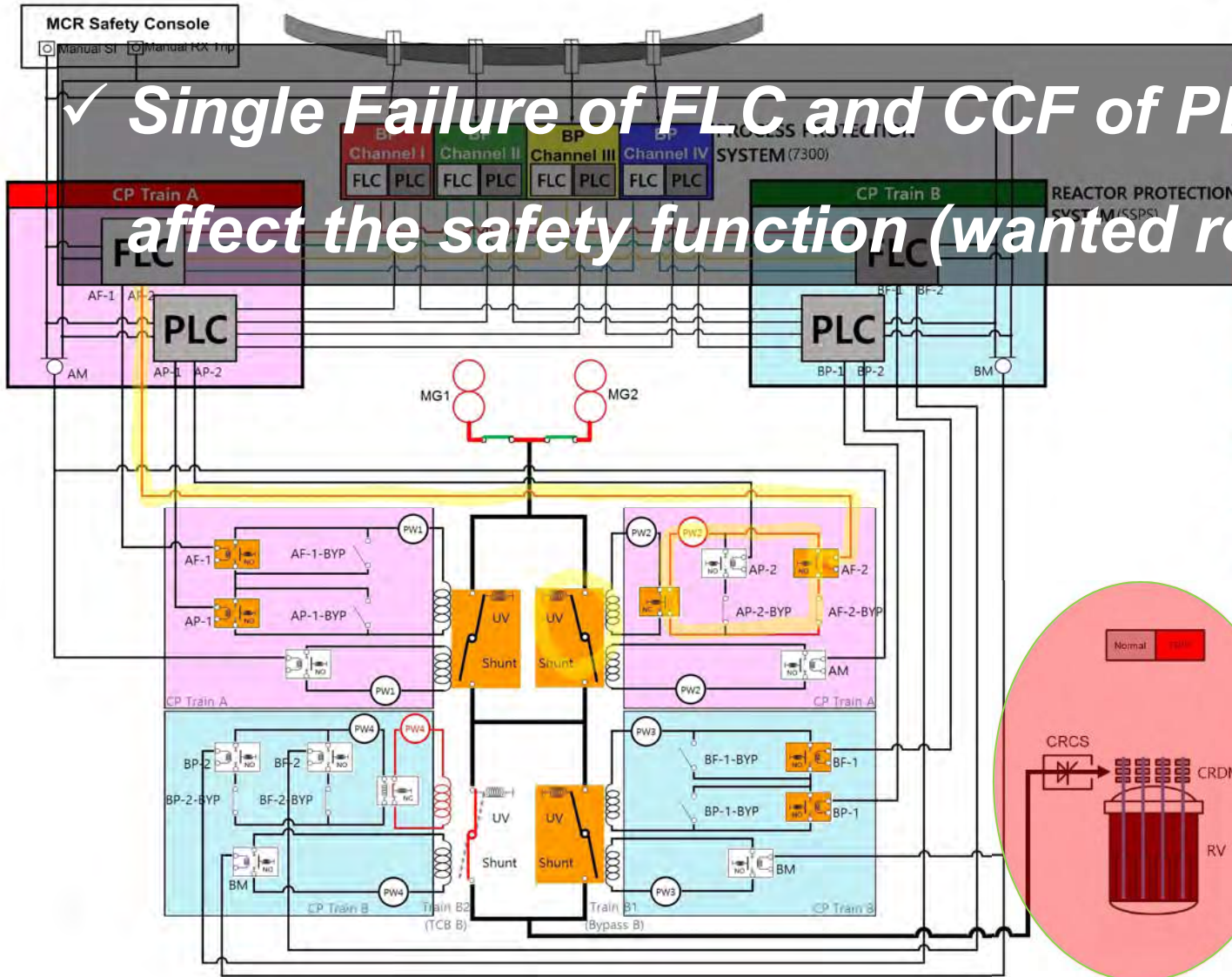
No photography of this exhibition  
Due to conservation and copyright restrictions.

Designed by DOOSAN Nuclear I&C Since 2016/11/3  
Patent No KR10-2016-0145468, US15/646611, CN201710532503.7,  
PH11-2017-000342 and BR10-2017-026123-9

# IV. Test Results of Protection system using Code Simulator

## - Countermeasure for CCF Issues

### ■ Case Study #4 Mitigate ATWS Under PLC CCF + FLC SPV



✓ *Single Failure of FLC and CCF of PLC does not affect the safety function (wanted reactor trip)*

ALARM			ESFAS
OP. ΔT RCT TRIP	PRZ HI PRESS RCT TRIP	PWR RANGE HI FLUX RCT TRIP	SIS
OP. ΔT RCT TRIP	PRZ LO PRESS & P-7 RCT TRIP	RCS FLOW LO AT HI PWR RCT TRIP	CIS-A
STMT PRESS RCT TRIP	SOURCE RANGE HI FLUX RCT TRIP	RCS FLOW LO AT HI PWR RCT TRIP	CIS-B
MANUAL RCT TRIP	INTMD RANGE HI FLUX RCT TRIP	SG 1,2,3 WTB LEVEL LO-LO RCT TRIP	CSS
MANUAL SI RCT TRIP	PWR RANGE HI FLUX HI SETPT RCT TRIP	TBN TRIP & P-7 RCT TRIP	FWIS
PRZ HI LEVEL RCT TRIP	PWR RANGE HI FLUX LO SETPT RCT TRIP	MSL PRESS LOW SI RCT TRIP	MSIS

CONTROL		PERMISSIVE	
C-1 High Neutron Flux Rod Stop Interlock	C-7 Loss of Load Interlock	P-4 Reactor Trip Permissive	P-11 Low Pressure Pressure SI Block Permissive
C-2 Overpower Rod Stop Interlock	C-8 Turbine Tripped Interlock	P-6 Source Range Block Permissive	P-12 High Steam Flow SI Block Permissive
C-3 OT.ΔT Rod Stop and Turbine Runback Interlock	C-9 Condenser Available Interlock	P-7 At-Power Permissive	P-13 Turbine At-Power Permissive
C-4 OP.ΔT Rod Stop and Turbine Runback Interlock	C-11 Control Bank D Rod Withdrawal Limit Interlock	P-8 Three Loop Flow Permissive	P-14 Steam Generator High Level Override
C-5 Low Power Interlock	C-16 Turbine Stop Loading Interlock	P-10 Nuclear At-Power Permissive	

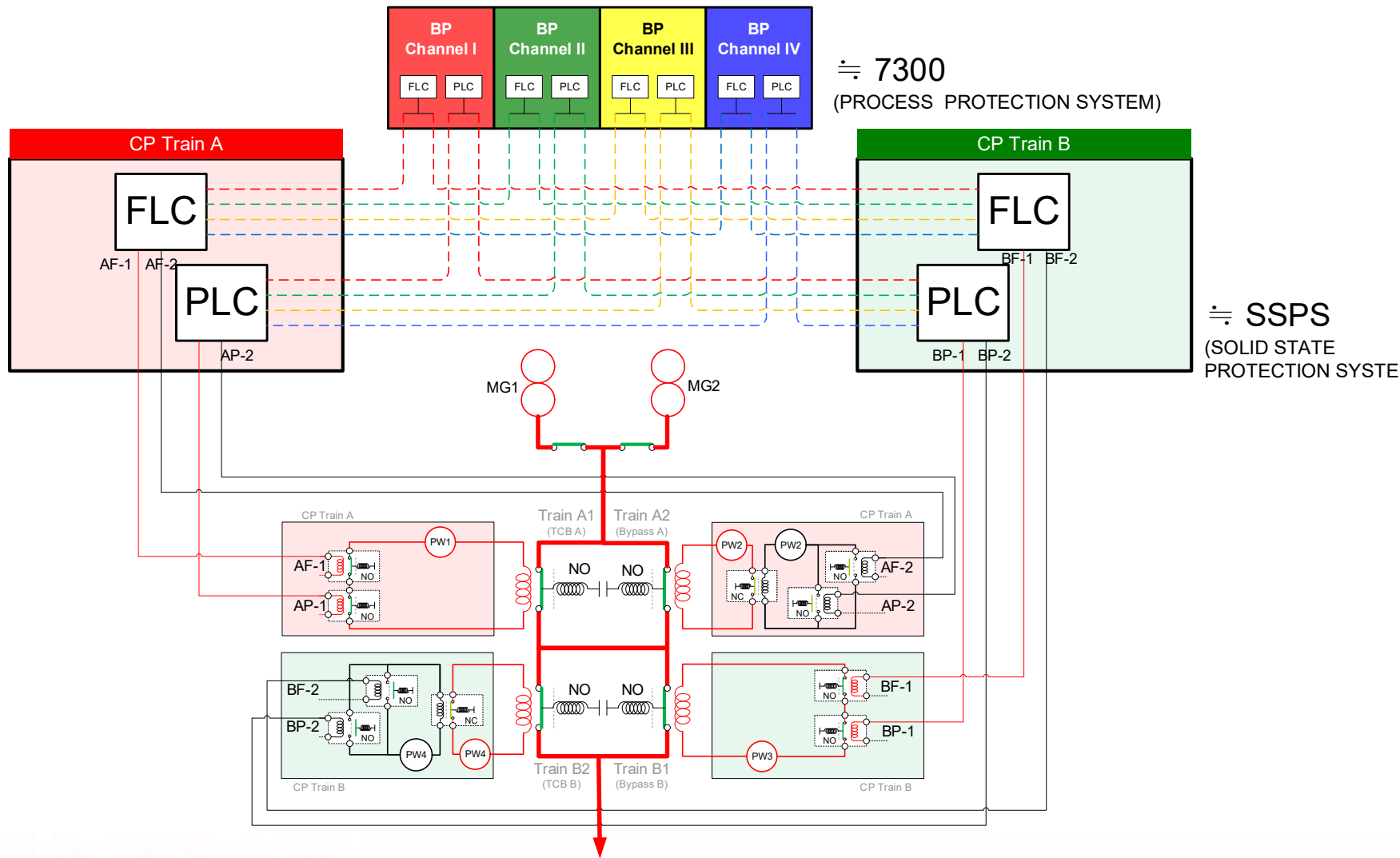
No photography of this exhibition  
Due to conservation and copyright restrictions:

Designed by DOOSAN Nuclear I&C Since 2016/11/3  
Patent No KR10-2016-0145468, US15/646611, CN201710532503.7,  
PH11-2017-000342 and BR10-2017-026123-9



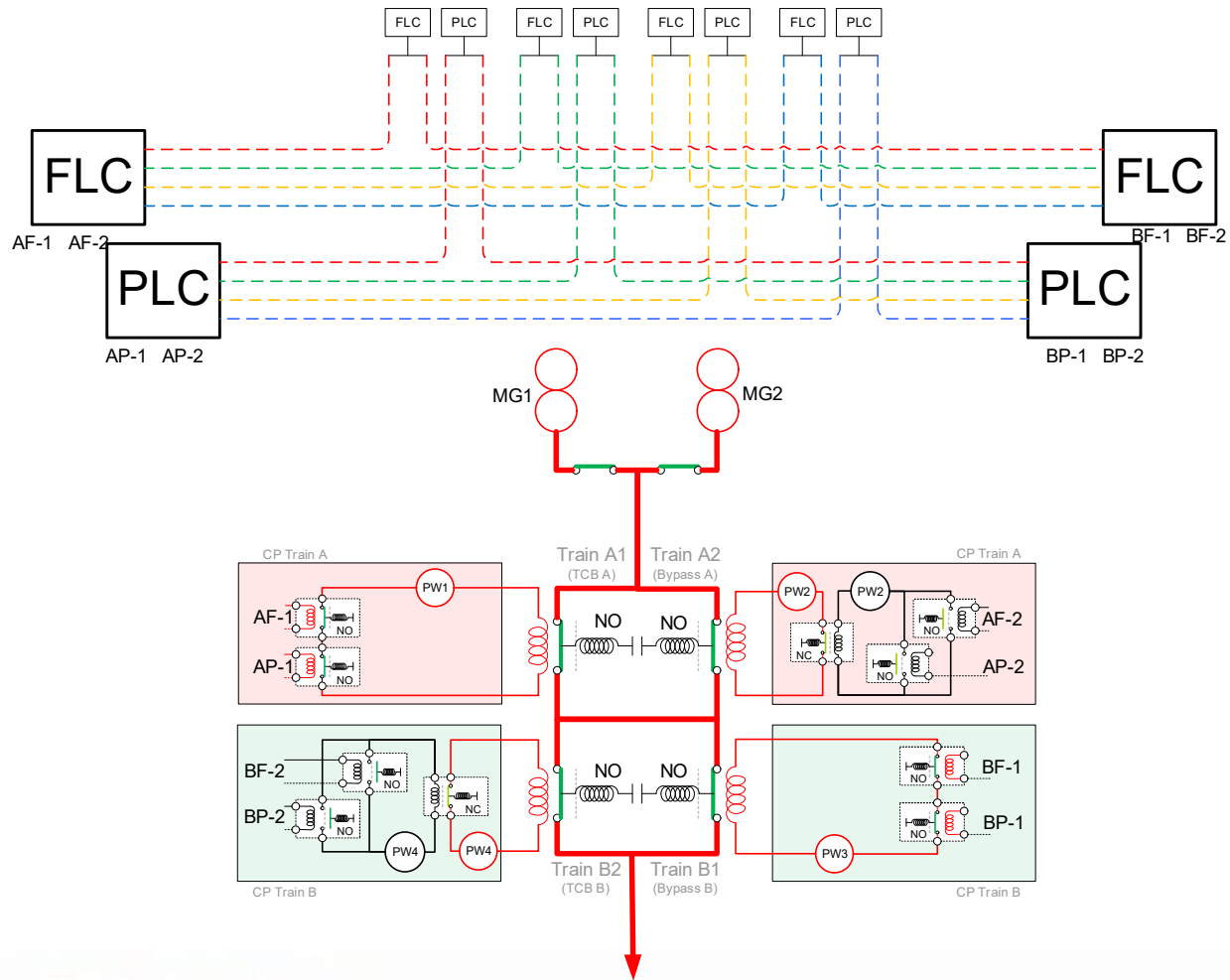
# V. Surveillance Test

## ■ Surveillance Test for Doosan Protection System



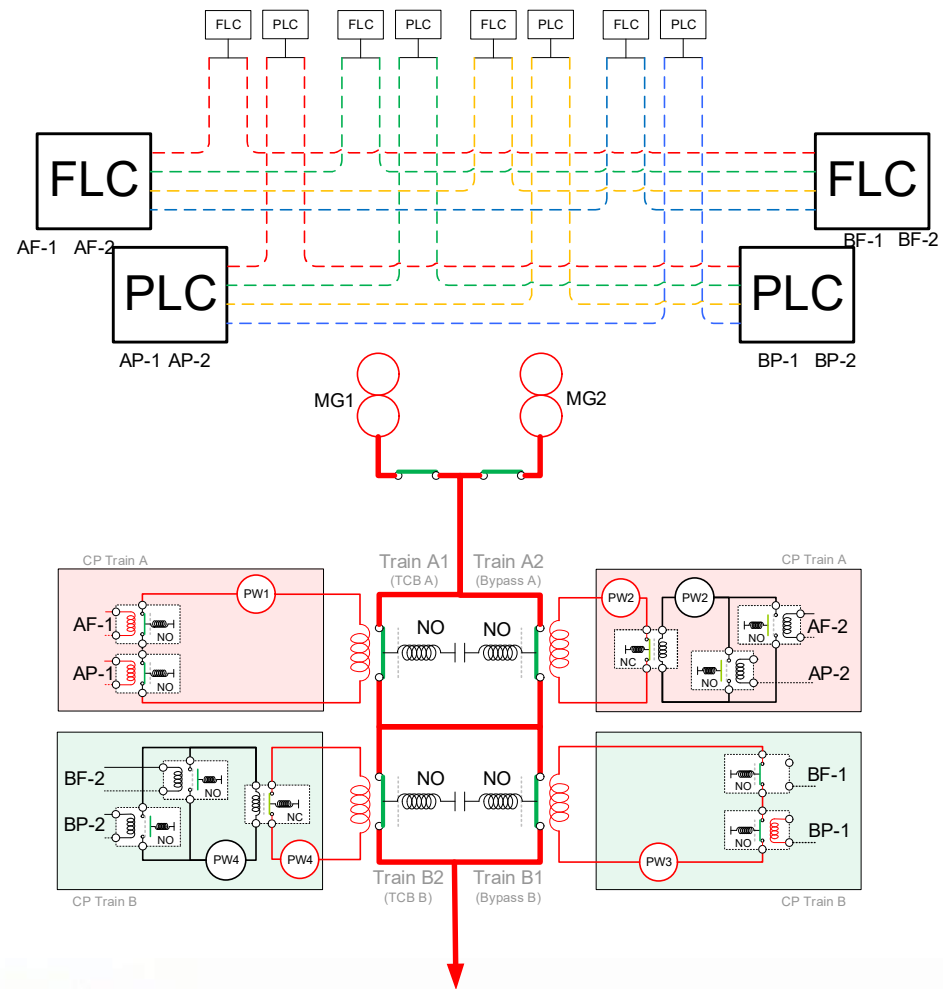
# V. Surveillance Test

## ■ Surveillance Test for Doosan Protection System



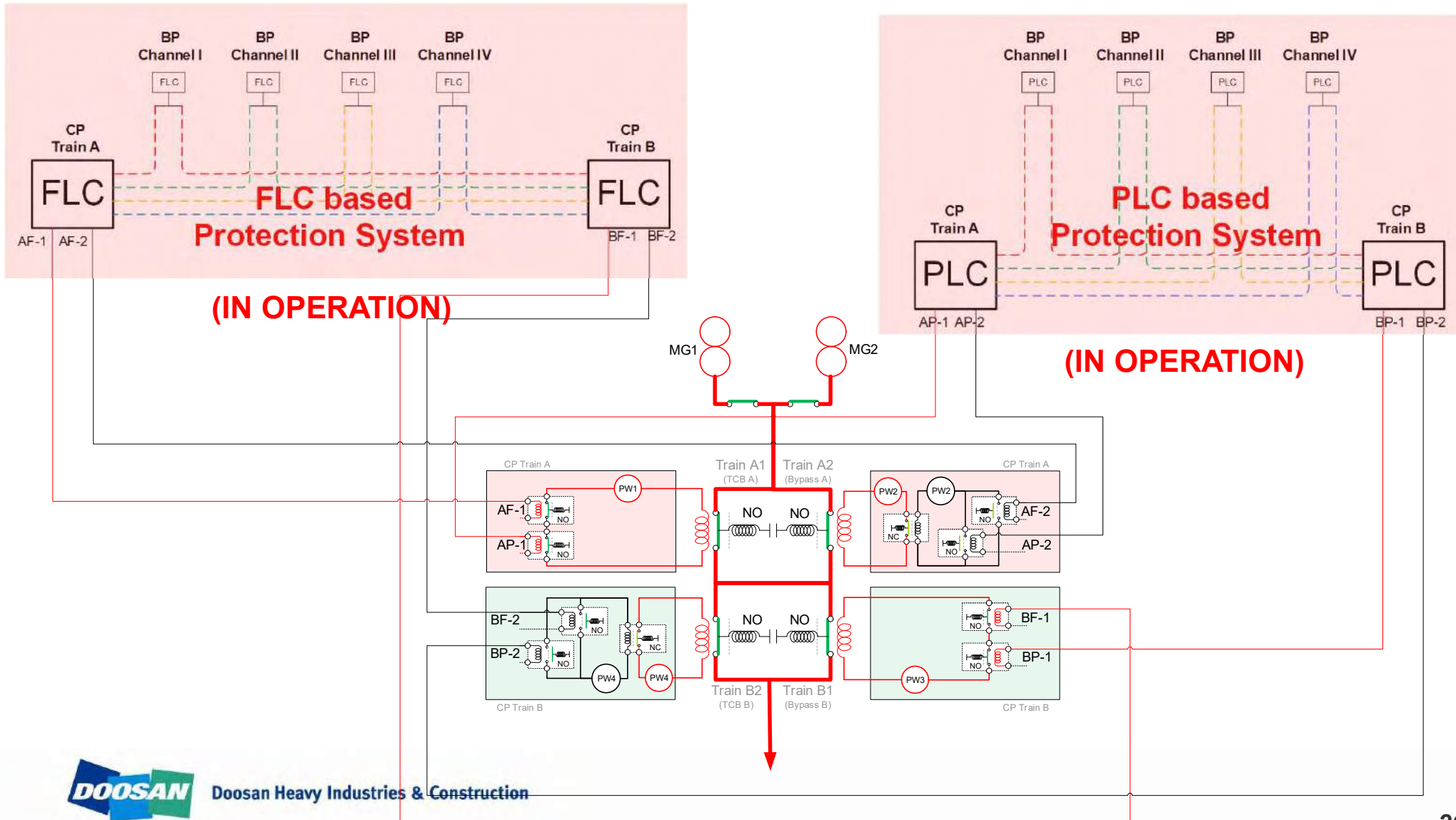
# V. Surveillance Test

## ■ Surveillance Test for Doosan Protection System



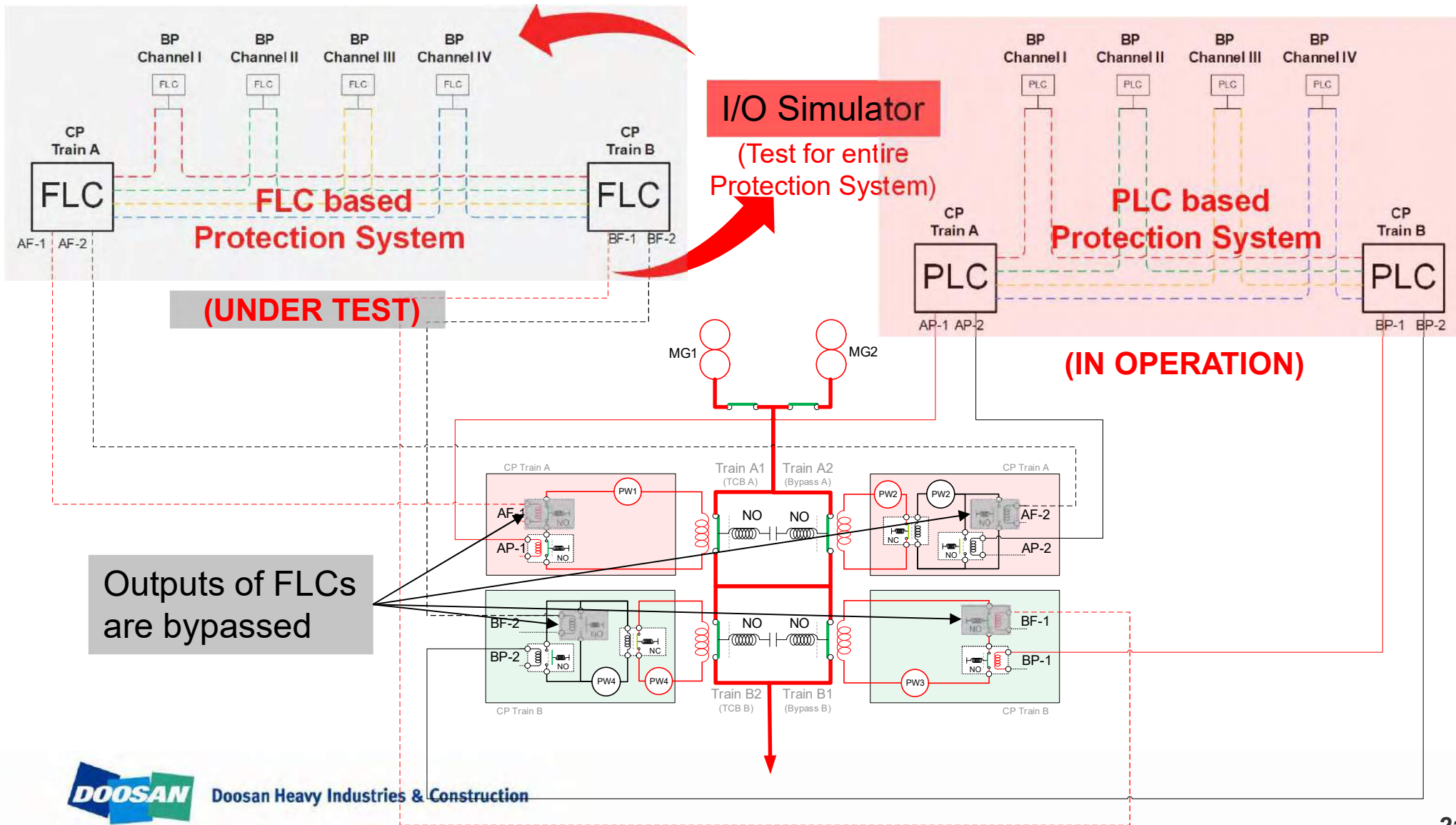
# V. Surveillance Test

## ■ Surveillance Test for Doosan Protection System



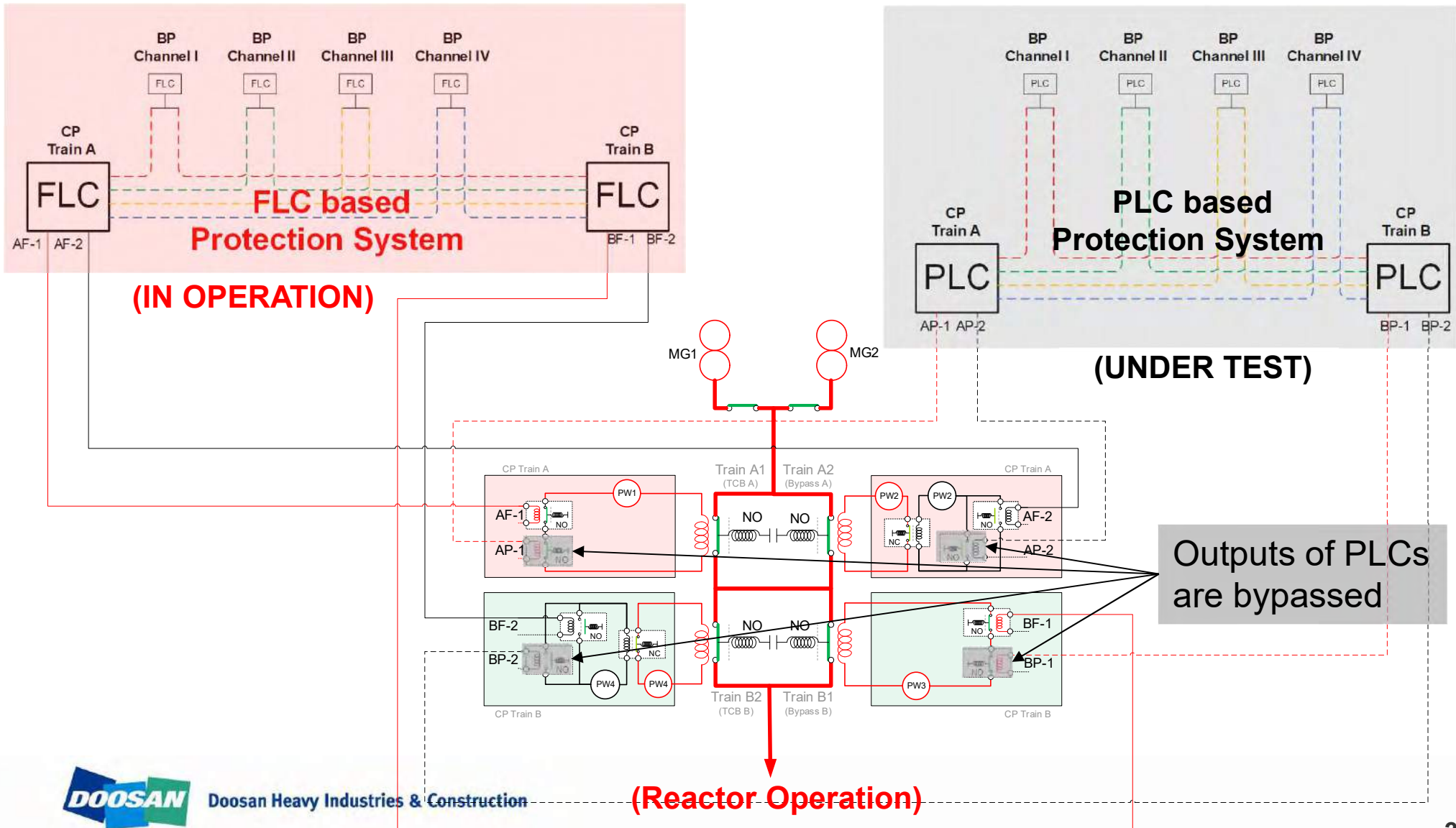
# V. Surveillance Test

## ■ Surveillance Test for Doosan Protection System



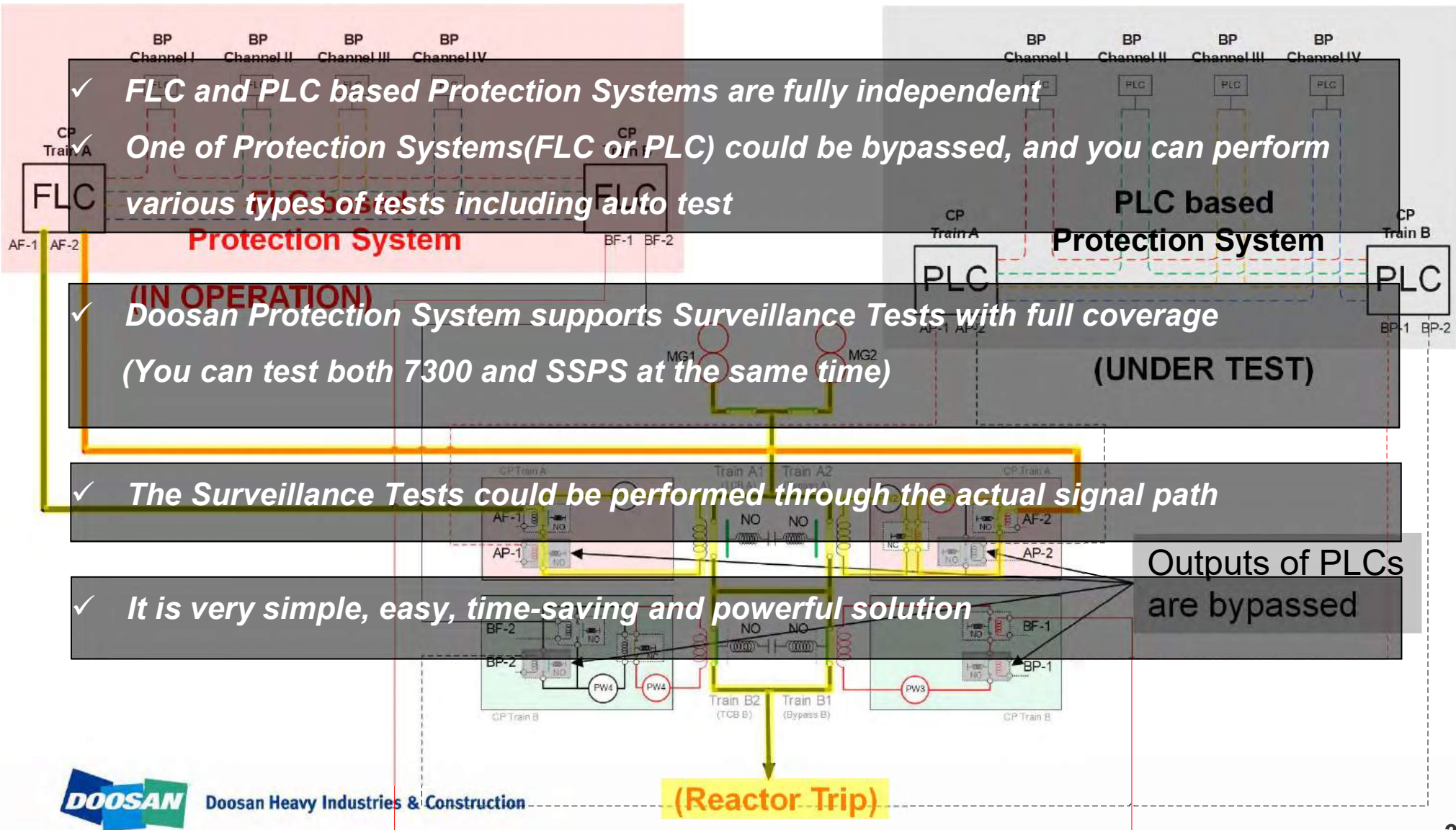
# V. Surveillance Test

## ■ Surveillance Test for Doosan Protection System



# V. Surveillance Test

## ■ Surveillance Test for Doosan Protection System

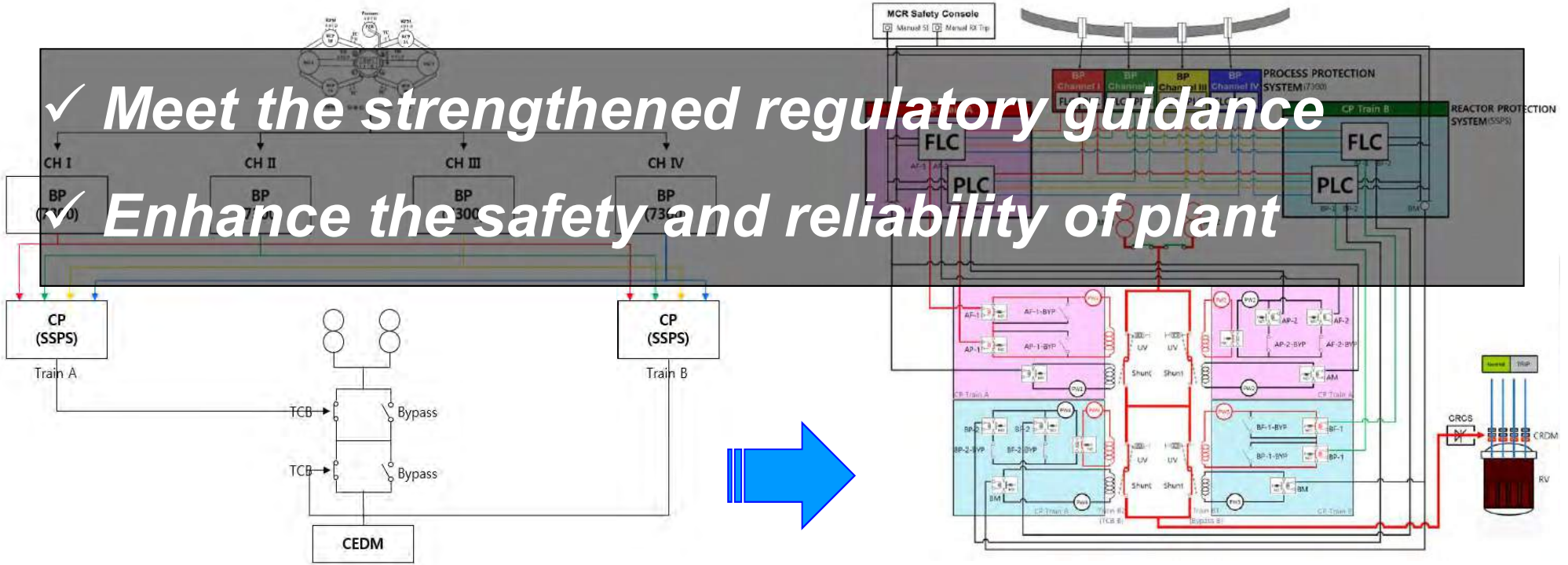


# VI. Conclusion

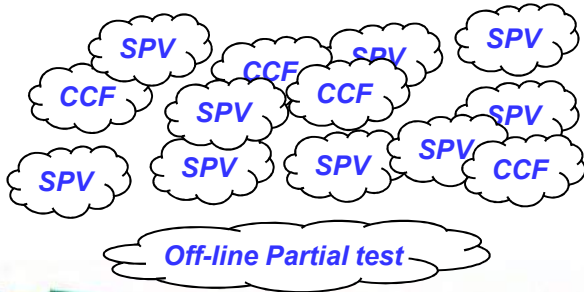
■ **FPGA Way is to enhance the Safety and Reliability of NPP**

✓ *Meet the strengthened regulatory guidance*

✓ *Enhance the safety and reliability of plant*



**As is : Old-designed system**



**To be : New designed system**





# Thank you



**Chaeho Nam**

**General Manger**

**Nuclear I&C, Doosan**

**Email : [chaeho.nam@doosan.com](mailto:chaeho.nam@doosan.com)**

**Phone : 82-31-270-7031**

**Cell : 82-10-4848-5683**



**Doosan Heavy Industries & Construction**