Application of Integrated Verification Approach to FPGA-based Safety-Critical I&C System of Nuclear Power Plant

Ibrahim Ahmed & Gyunyoung Heo
Department of Nuclear Engineering, Kyung Hee University, Yongin-si, Korea
Jaecheon Jung
KEPCO International Nuclear Graduate School, Ulsan, Korea

October 26-28, 2016

Contents

- ❑Introduction
- ❑Methodology
- ❑Results
- ❑Conclusions

Introduction (1/2)

- Safety-critical I&C system in nuclear power plant (NPP) implemented on programmable logic controllers (PLCs) plays a vital role in safe operation of the plant – **RPS**.

- The challenges such as
  - fast obsolescence,
  - the vulnerability to cyber-attack, and other related issues of software systems

- have currently led to the consideration of field programmable gate arrays (FPGAs) as an alternative to PLCs because of their advantages and hardware related benefits.

- Safety analysis for FPGA-based I&C systems, and verification and validation (V&V) assessments still remain important issues to be resolved, which are now become a global research point of interests.

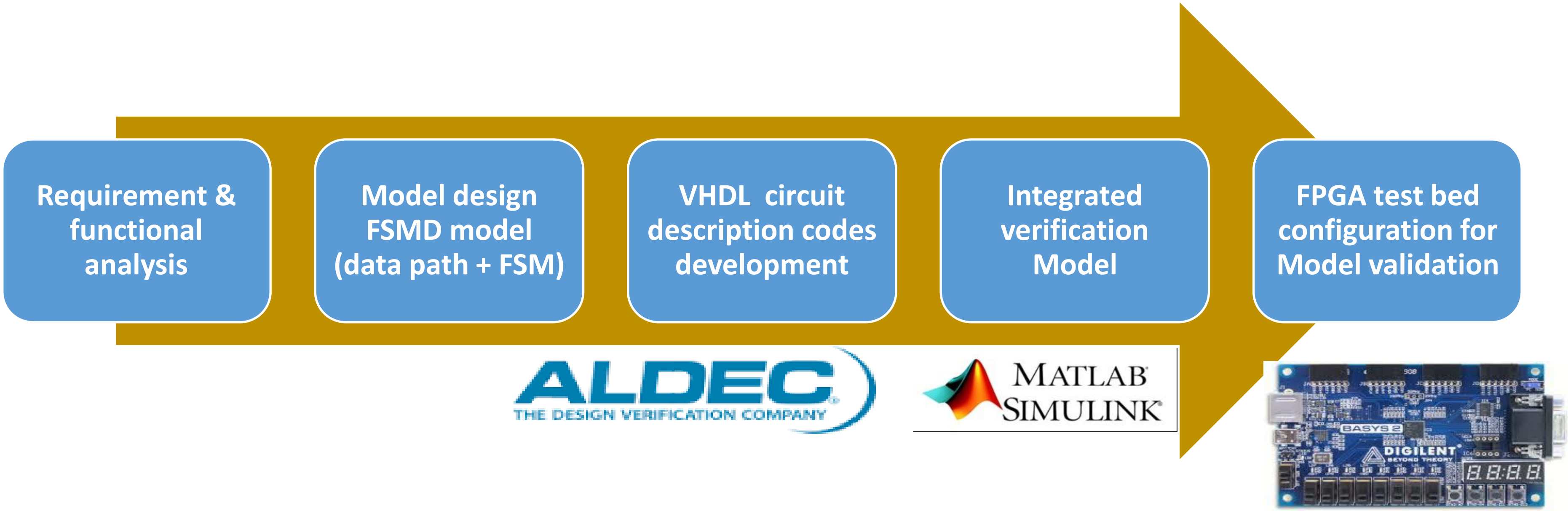
- The regulations and standards demand that sufficient V&V should be performed to demonstrate the safety level of the systems.

Introduction (2/2)

- In FPGA design verification, the designers make use of verification techniques by writing the test benches.
  - ➢ It involved various stages of verification activities of register-transfer level (RTL), gate-level, and place and route.
- Writing the test benches is time consuming and require a lot of efforts to achieve a satisfied desire results.
- Performing the verification at each stage is a major bottleneck and demanded much activities and time.
- In addition, verification is conceivably, the most difficult and complicated aspect of any design.
- **In view of these, this work applied an integrated verification approach to the verification of FPGA-based I&C system in NPP that**
  - ➢ **Simultaneously verified the whole design modules using MATLAB/Simulink HDL Co-simulation models.**

Methodology (1/5)

❑ ***Research Approaches***



Requirement & functional analysis

Model design FSMD model (data path + FSM)

VHDL circuit description codes development

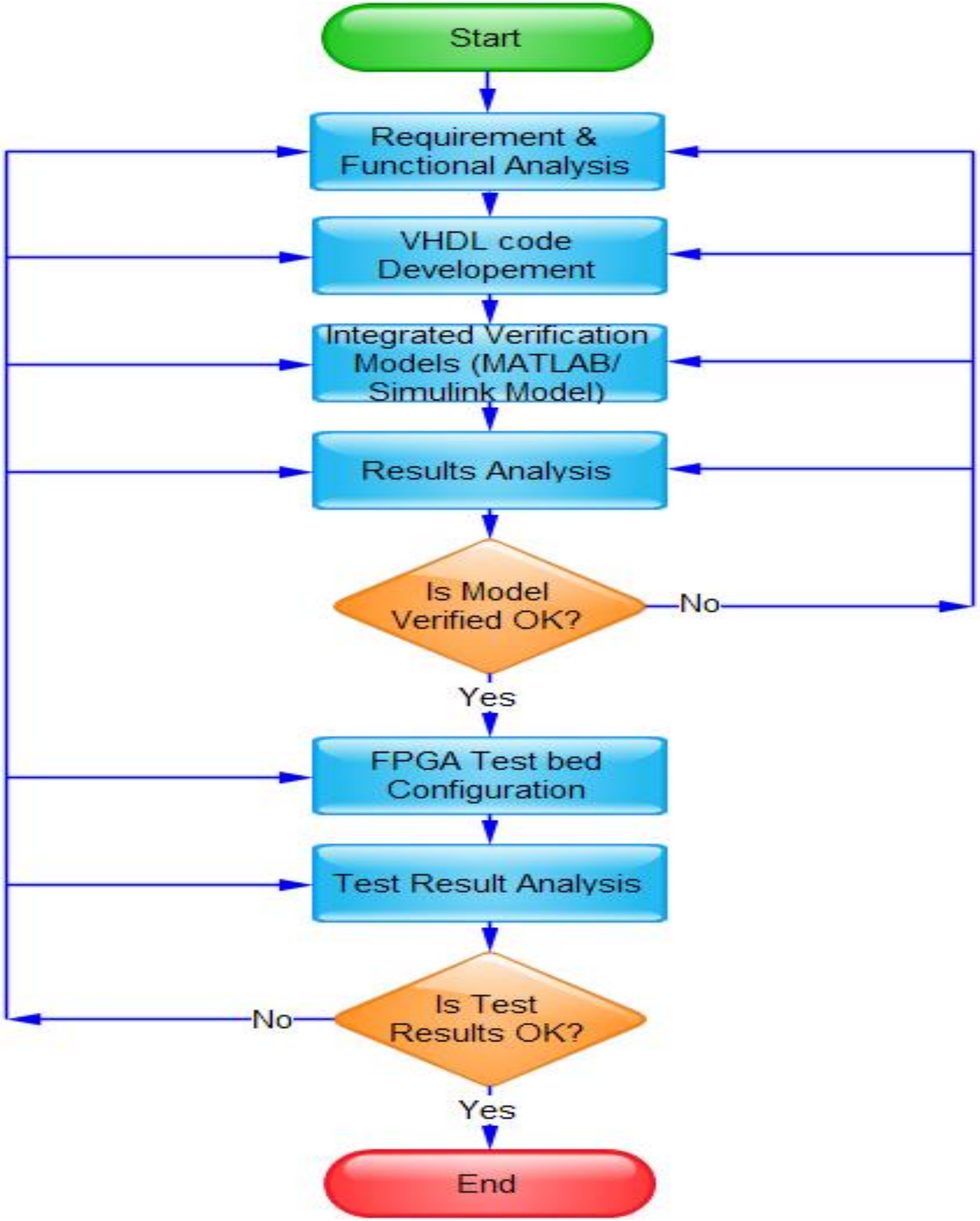
Integrated verification Model

FPGA test bed configuration for Model validation

Methodology (2/5

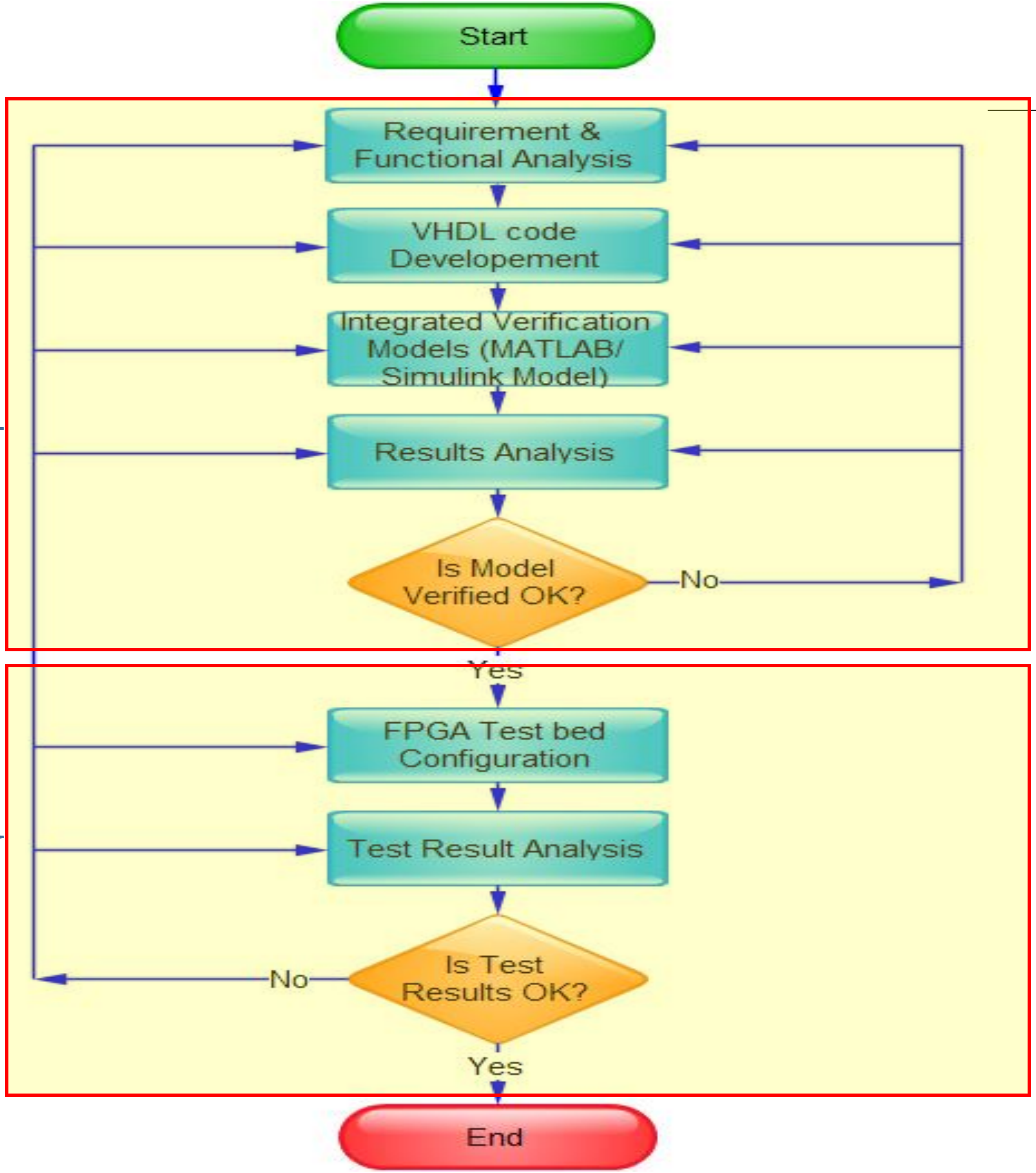
❑ *Research Approaches*

Model Development Flowchart



Methodology (2/5

❑ *Research Approaches*

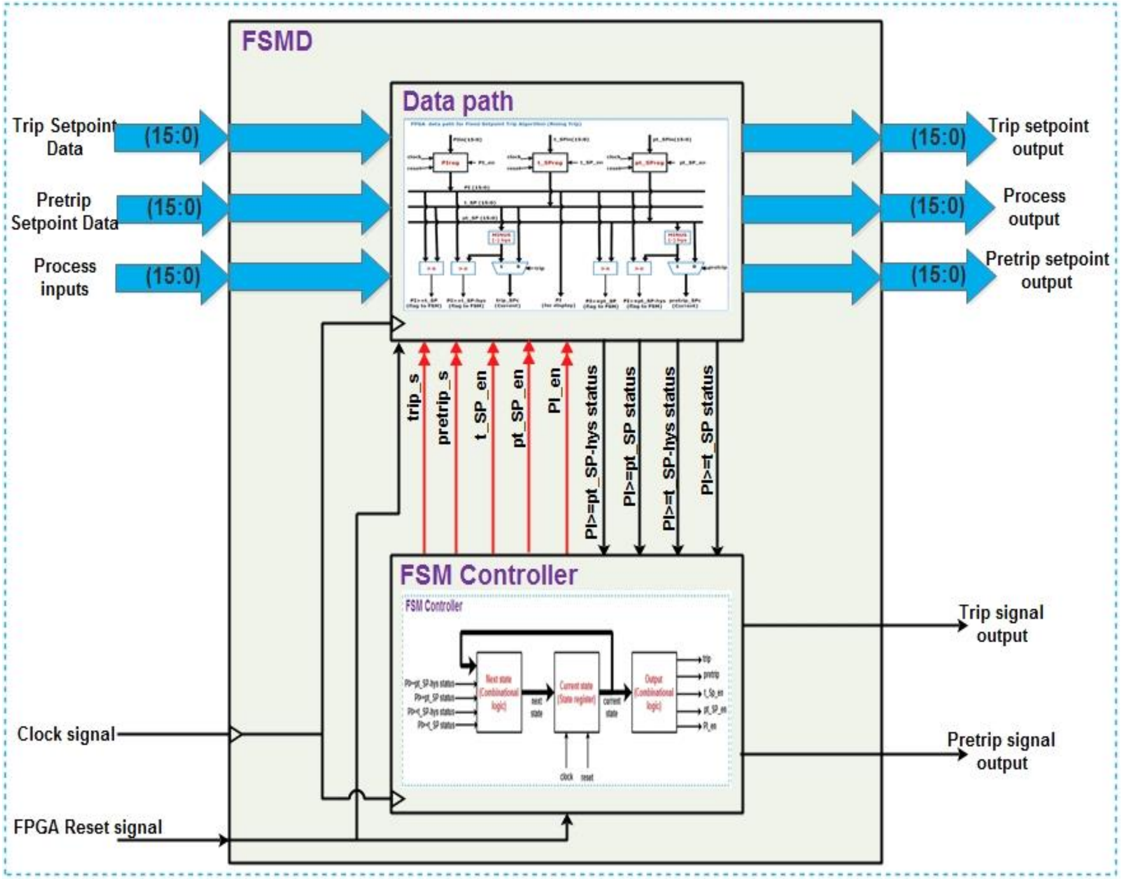


Development & Verification Phases

Validation Phases

Methodology (3/5)

❑ *VHDL Code Development Model*



FSMD Model for FSP trip Algorithms

VHDL modules

- ● **Unit 1**
- ● **Unit 2**
- ● **Unit 3**

Methodology (4/5)

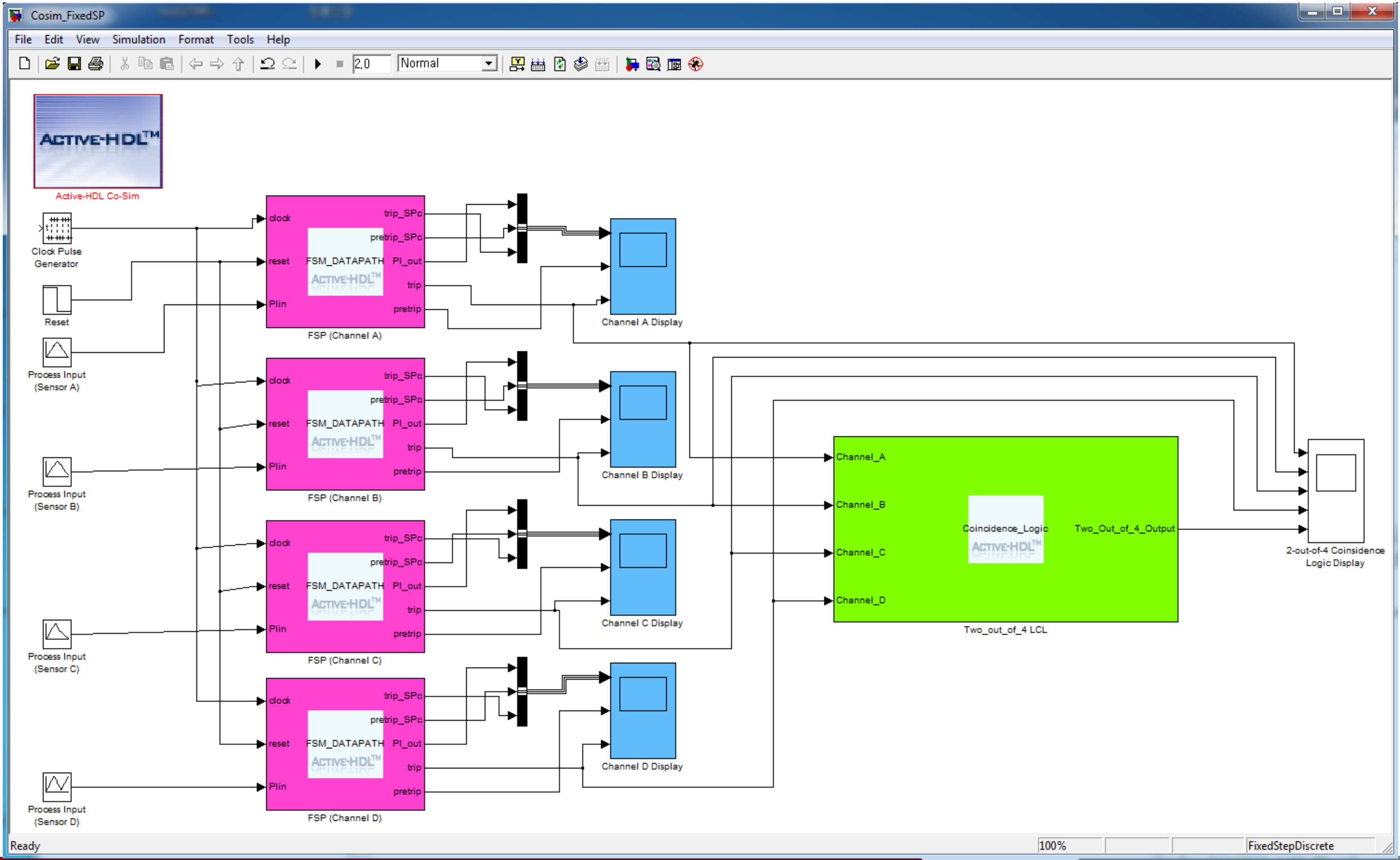
❑ *Integrated Verification Model*

- The verification and testing of the FPGA-based trip logic (for example, the case of fixed setpoint logic) involves checking and observing the following RTL/gate-level code structures:
  - ➢ The comparator logics are correctly implemented – the hysteresis is applied to the setpoint when the system process is in the expected level.
  - ➢ The trip and pretrip logics are properly and correctly implemented – the logics respectively generate trip and pretrip signals when the process input exceeds the predefined limits.
  - ➢ The behavior of the trip algorithm at every point is correct – that is, each logic performs the task it is designed for and does not compromise the performance of the other logics.
  - ➢ The two-out-four coincidence logic provides correct trip/pretrip output if at least two out of four channels issue the trip signal.
  - ➢ The FPGA-based safety-critical I&C system satisfies the requirements of the fixed setpoint algorithm while it is in operation.

Methodology (5/5)

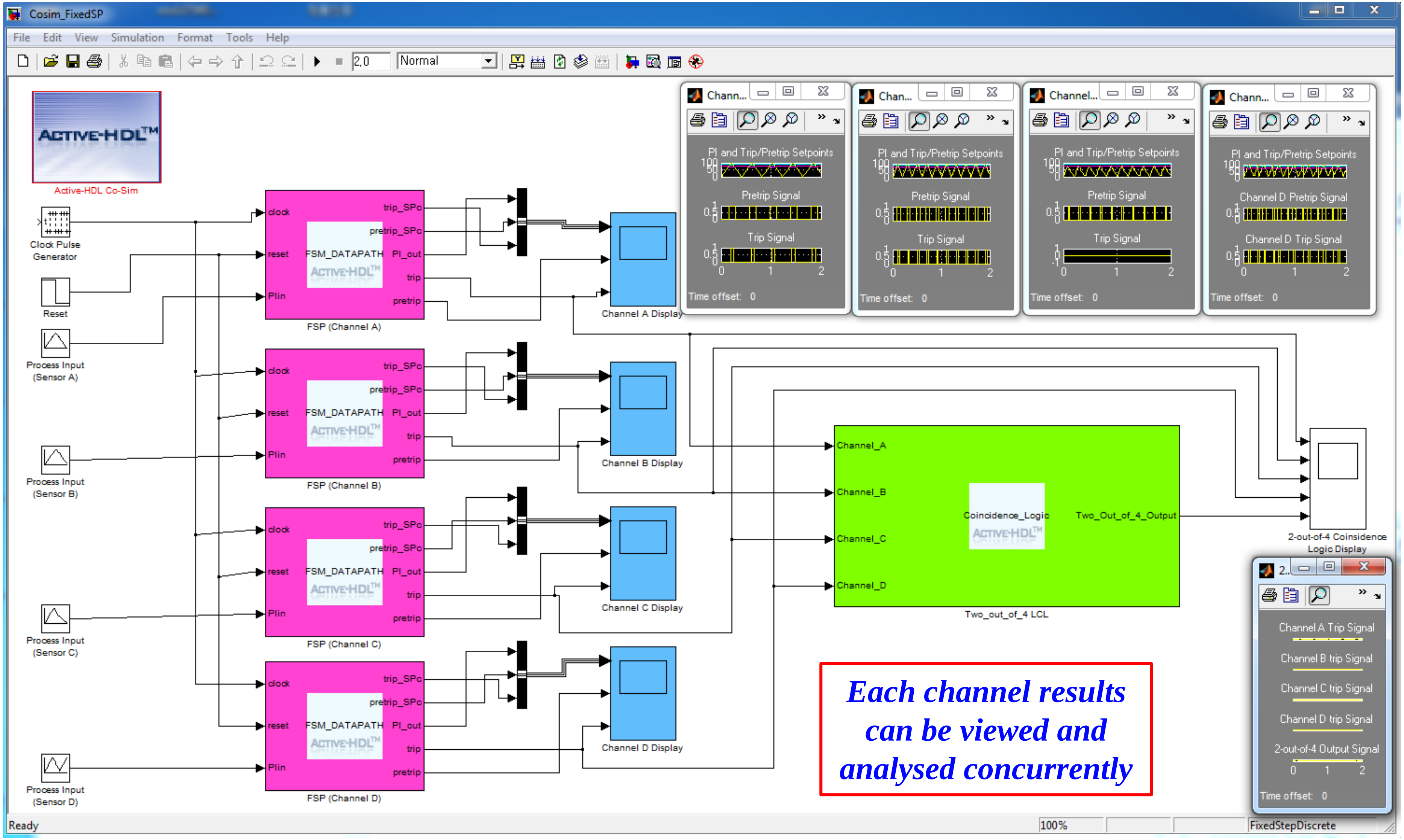
❑ *Integrated Verification Model*

- Simulink model for integrated verification test (4 channels RPS with a coincidence logic)



Results (1/4)

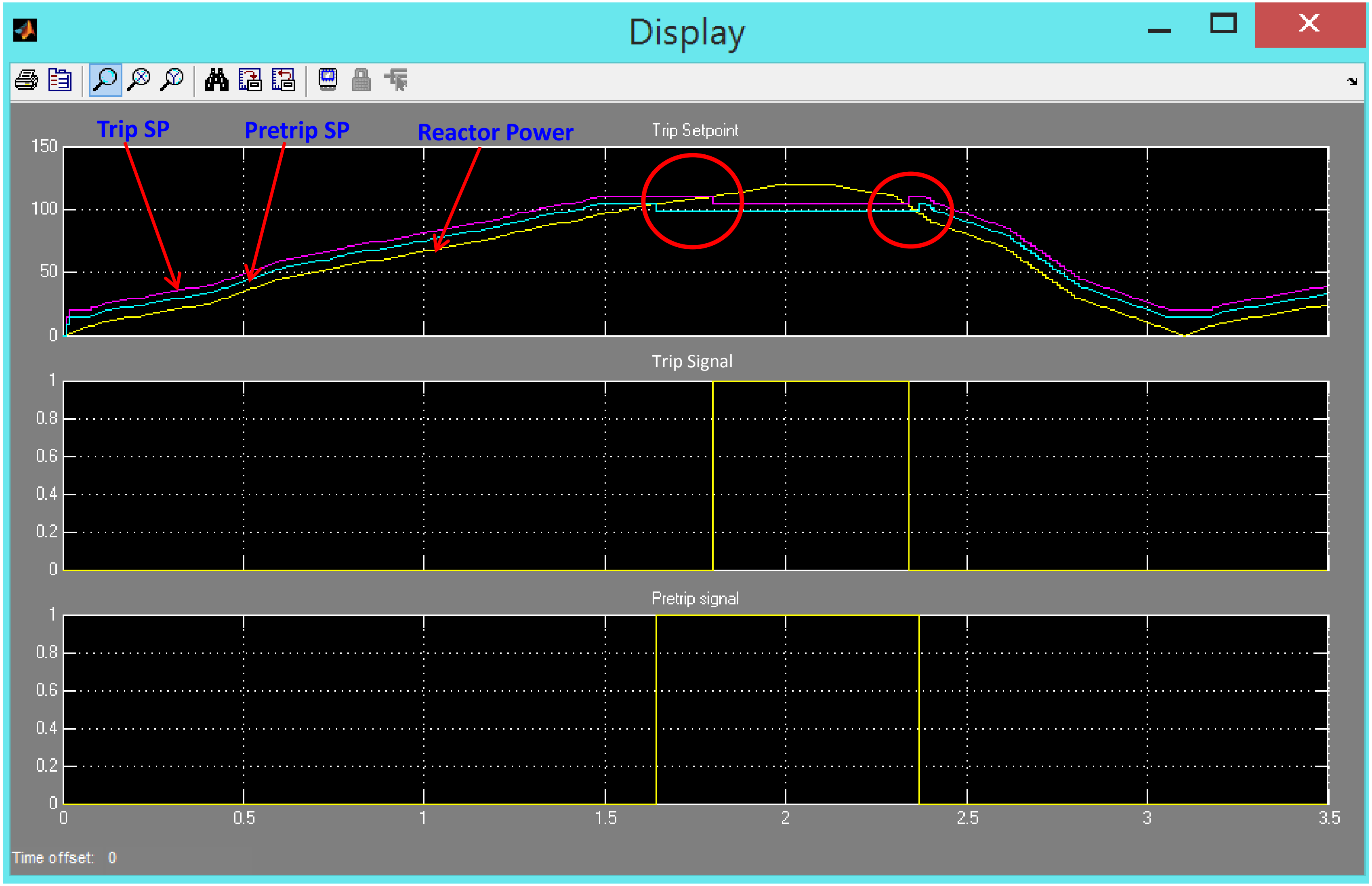
- Integrated verification results of four channels FPGA-based PPS.



Each channel results can be viewed and analysed concurrently

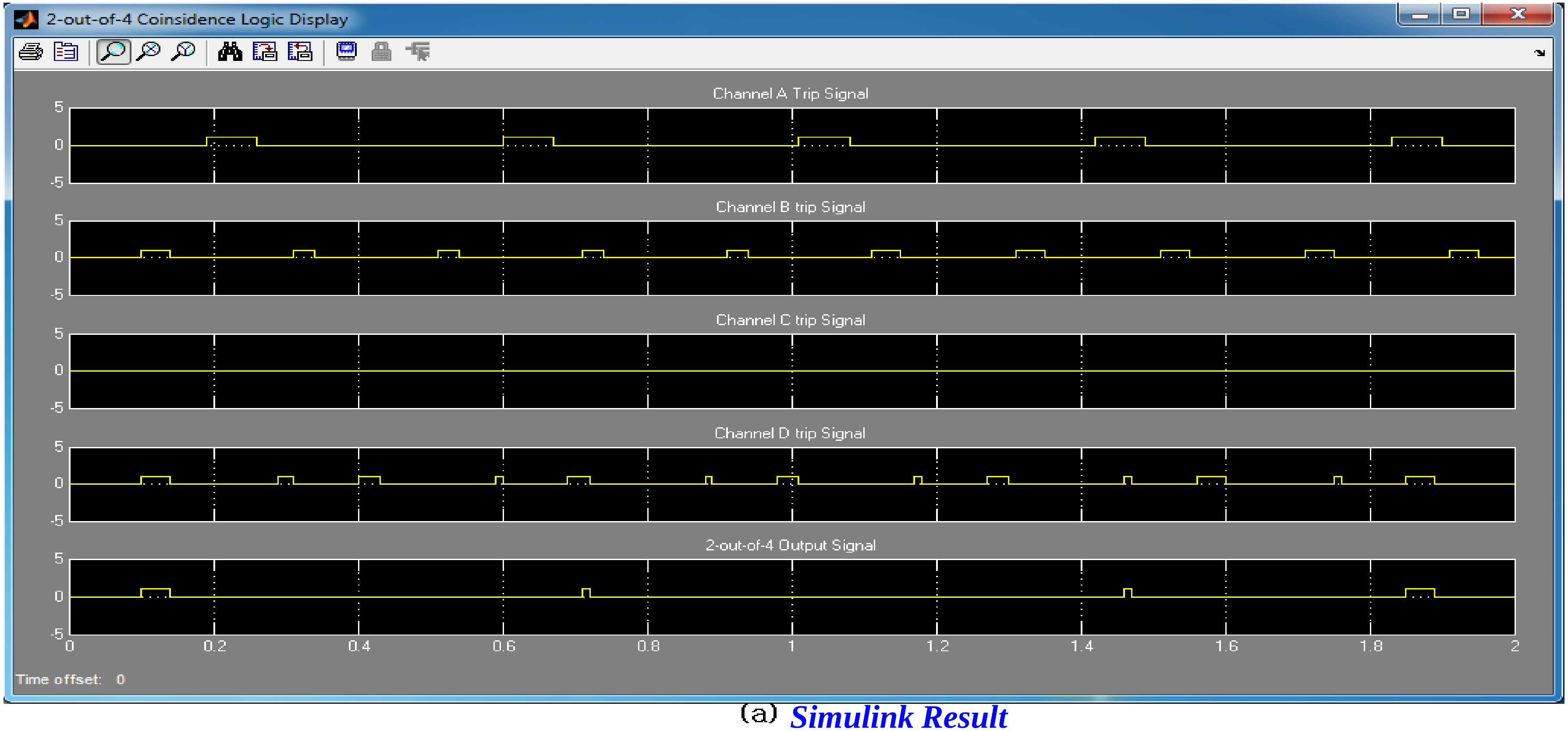
Results (2/4)

- Integrated verification results of Variable Overpower Trip (VOPT).

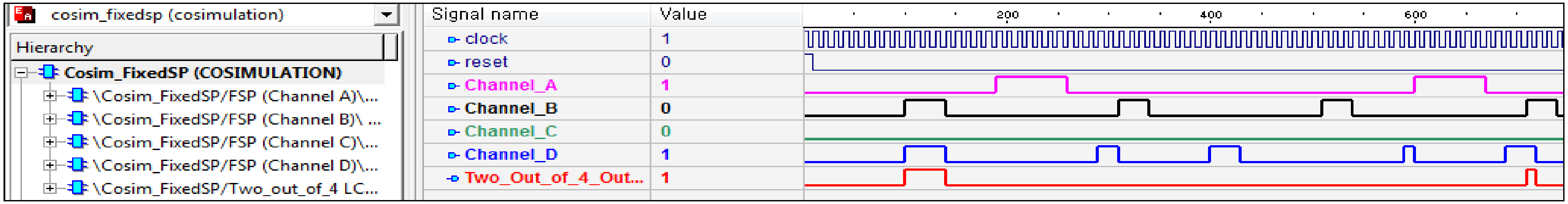


Results (3/4)

- Integrated verification results of four channels FPGA-based PPS.



(a) ***Simulink Result***



cosim_fixedsp (cosimulation)
Hierarchy
Cosim_FixedSP (COSIMULATION)
\Cosim_FixedSP/FSP (Channel A)\...
\Cosim_FixedSP/FSP (Channel B)\ ...
\Cosim_FixedSP/FSP (Channel C)\...
\Cosim_FixedSP/FSP (Channel D)\...
\Cosim_FixedSP/Two_out_of_4 LC...
200
400
600

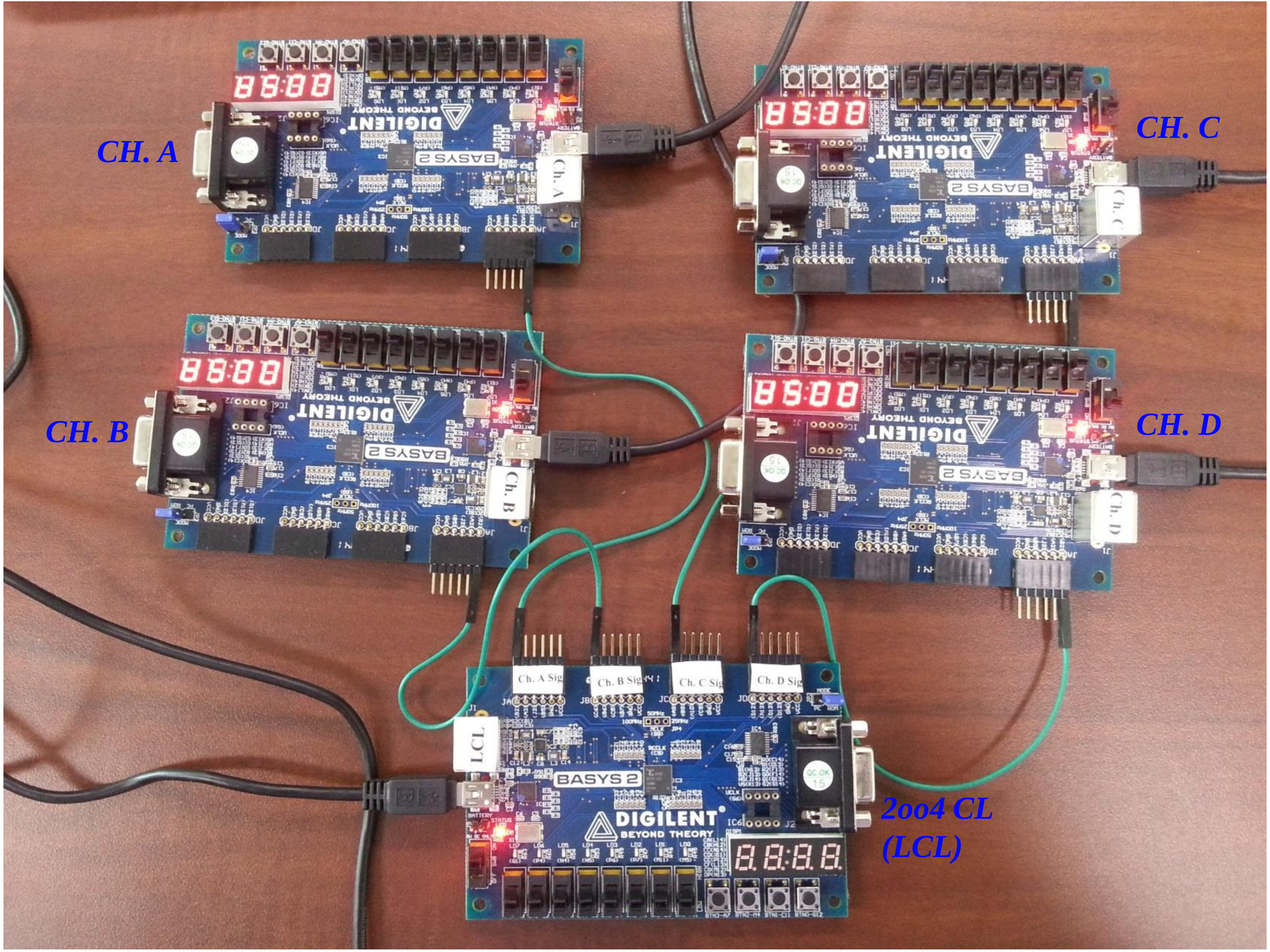
Signal name	Value
clock	1
reset	0
Channel_A	1
Channel_B	0
Channel_C	0
Channel_D	1
Two_Out_of_4_Out...	1

(b) ***Co-sim on Active-HDL***

Results (4/4)

- Integrated verification results of four channels FPGA-based PPS.

FPGA test bed is configured for validation test.



Conclusions

- Verification is the most difficult and complicated aspect of any design, and an FPGA design is not an exception.
- Therefore, in this work, we introduced and discussed how an application of integrated verification technique to the verification and testing of FPGA-based I&C system design in NPP can
  - ➢ facilitate the verification processes, and
  - ➢ verify the entire design modules of the system simultaneously
- using MATLAB/Simulink HDL co-simulation models.
- Conclusively, the results showed that, the integrated verification approach through MATLAB/Simulink models, if applied to any design to be verified, could speed up the design verification and reduce the V&V tasks.
- This is because the entire FPGA-based system design modules to be verified are modeled collectively, and the test cases and test scenarios are from the Simulink models which are easy to be developed compare with writing test benches using any of the HDL languages.

Thank You