2024 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

MUNICH, GERMANY
OCTOBER 15-16, 2024

Trustworthiness Evaluation of Deep Learning Accelerators Using UVM-based Verification with Error Injection

Randa Aboudeif*†, Tasneem A. Awaad‡, Mohamed AbdElsalam†, Yehea Ismail*

*Electronics and Communications Engineering Department, The American University in Cairo, Cairo, Egypt

†Siemens Digital Industries Software, Cairo, Egypt

‡Department of Computer and Systems Engineering, Faculty of Engineering, Ain Shams University, Cairo, Egypt

The American University in Cairo

Faculty of Engineering - Ain Shams University 1839

SIEMENS

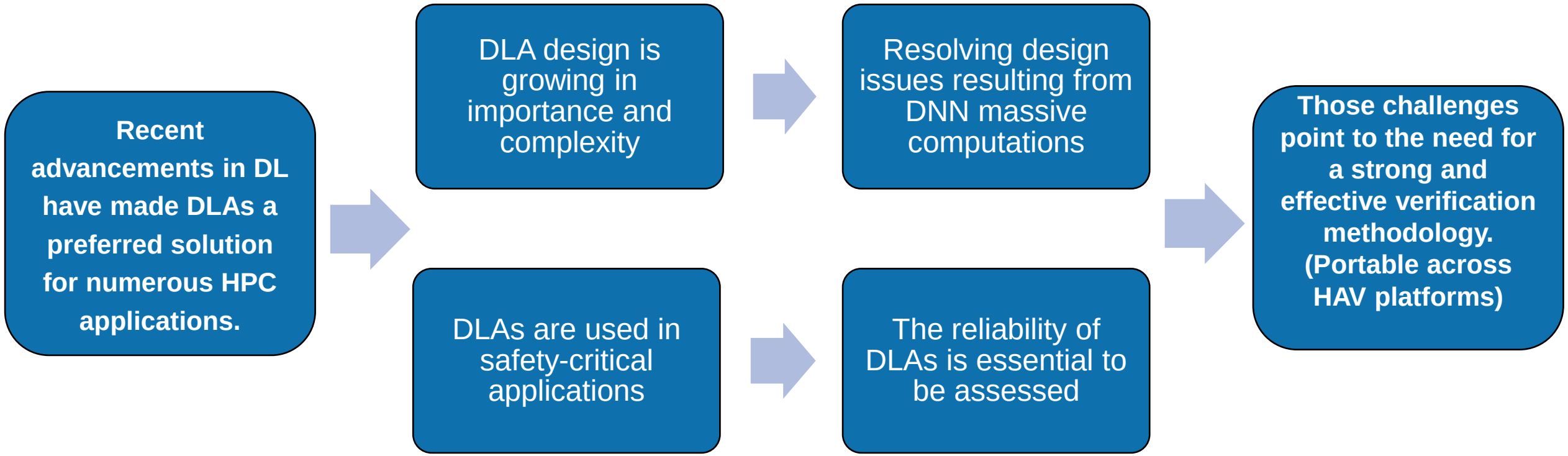
accellera SYSTEMS INITIATIVE

Agenda

- ❑ **Introduction**
- ❑ **Contribution**
- ❑ **Proposed UVM-based Verification Framework**
- ❑ **NVDLA Case Study**
- ❑ **Experimental Results**
- ❑ **Conclusion**
- ❑ **Future Work**

Introduction

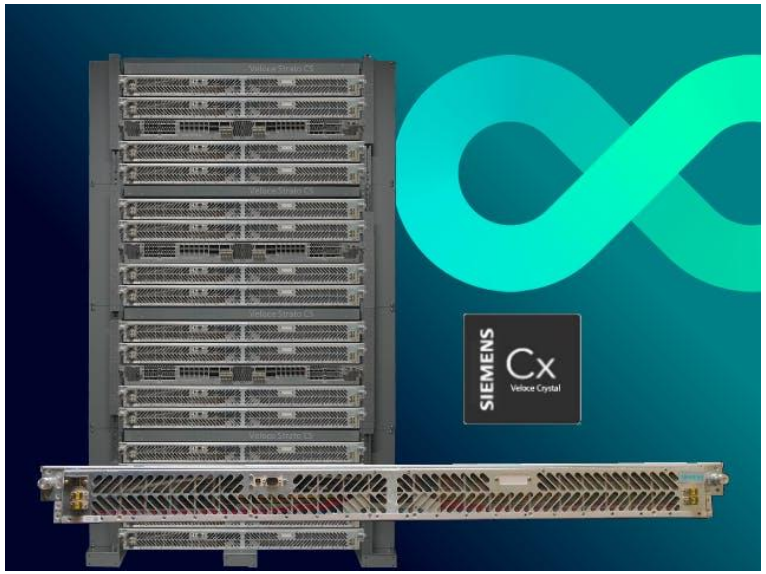
Introduction



Introduction

HAV Platform includes Emulation and prototyping platforms

- Emulation platforms



https://eda.sw.siemens.com/en-US/ic/veloce/strato-hardware/

- FPGA prototyping platforms

https://newsroom.sw.siemens.com/en-US/mips-veloce-profpga/

Introduction

- All the related previous work applies error injection for a specific DLA design without using UVM or for a specific DNN architecture.
  - Investigating the resilience of neural network accelerator RTL design is using a HLS based methodology for applying fault injection into the data registers of the RTL neural network accelerator.
  - Fault injection technique is done for four popular neural networks for image recognition using “Tiny-CNN” with a C++ model for the DLA.
- The proposed error injection methodology is scalable and reliable across different DLA designs and DNN architectures, and portable across the various HAV platforms to accelerate the verification process.

Contribution

- Implementing a cross-layer error injection methodology using three error injection mechanisms:
  - Applying error injection in the DNN data path.
  - Applying adversarial attacks on the CNN input image.
  - Applying error injection in the DLA hardware configuration registers.

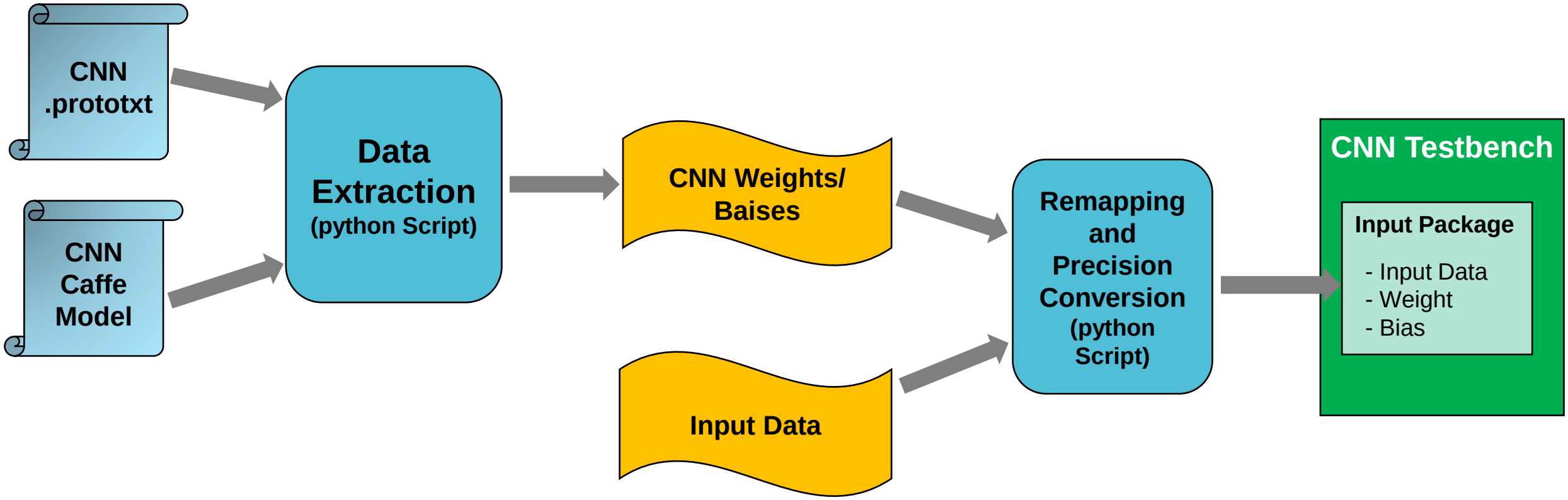
Contribution

- Applying the proposed framework on NVDLA as a case study.
- It is portable across simulation, and Hardware Assisted Verification (HAV) platforms.

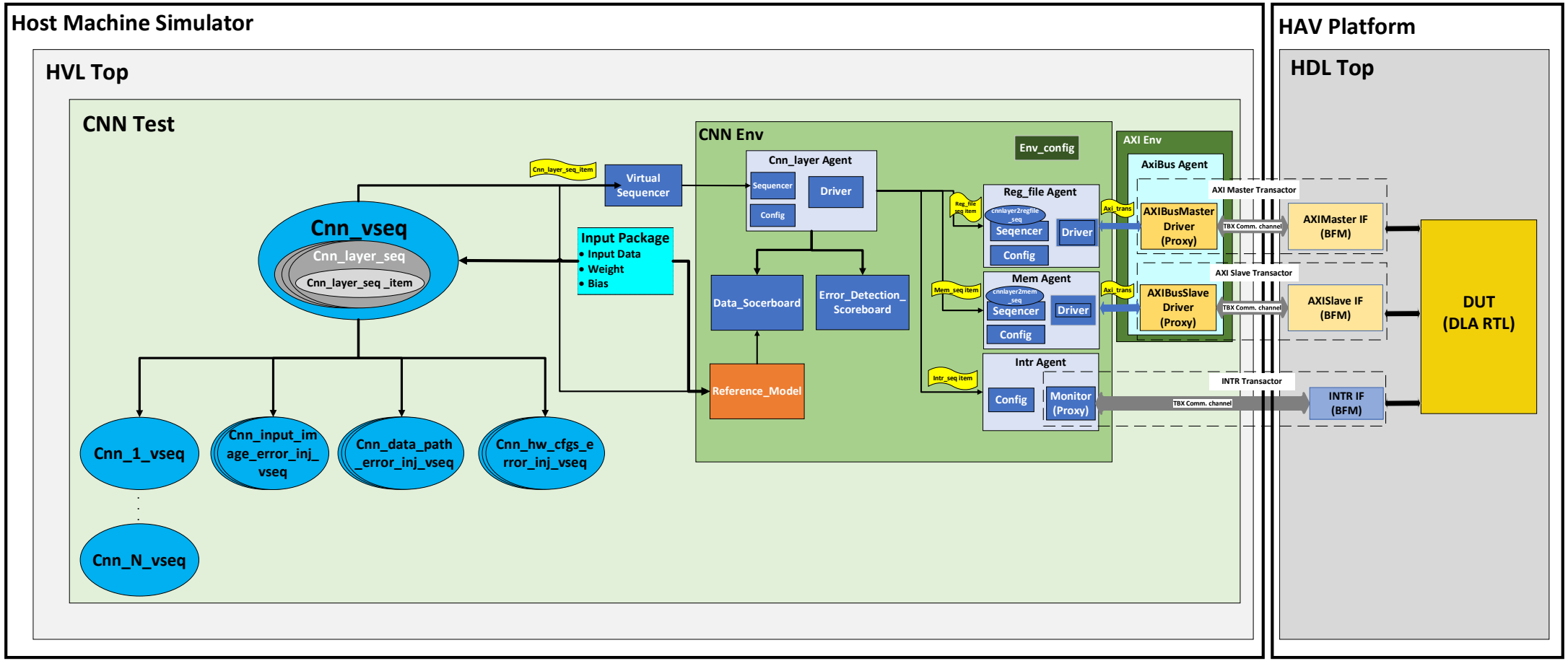
To the best of our knowledge, this is the first contribution to verifying DLAs using generic and reusable UVM testbench with Error Injection capability

Proposed UVM-based Verification Framework

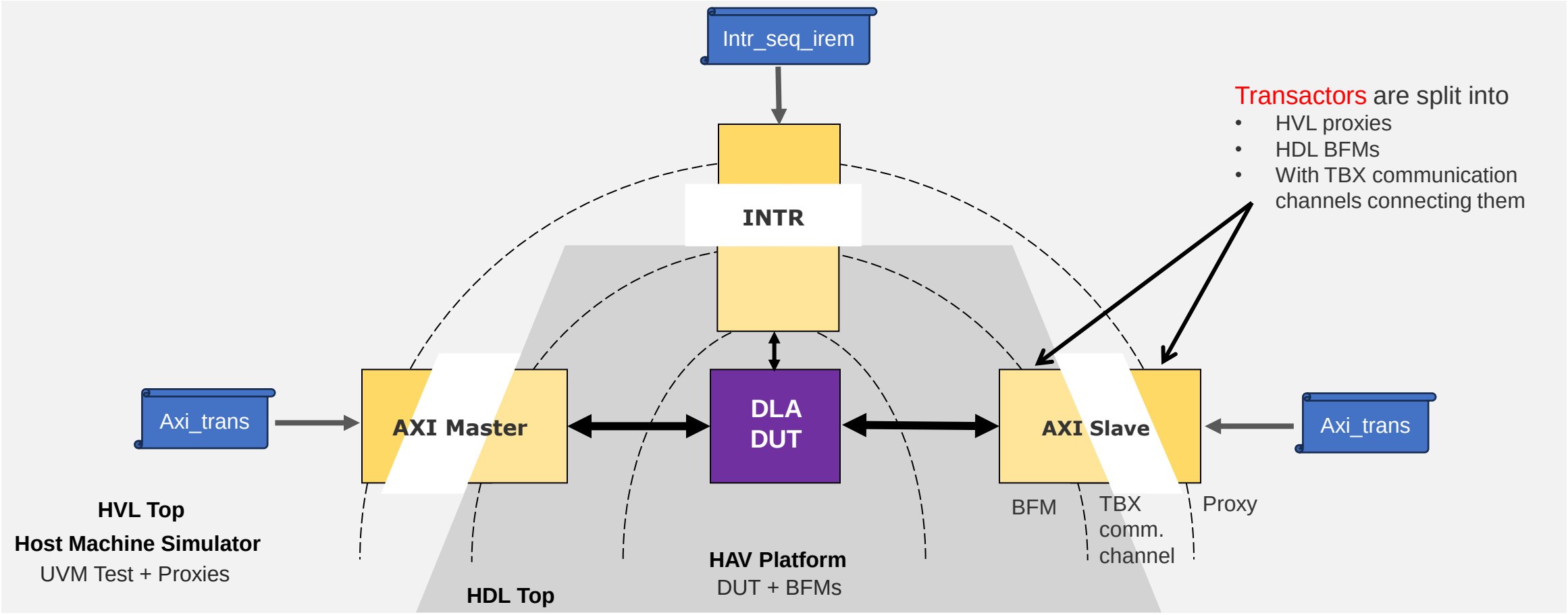
Input Data and Weight Preparation



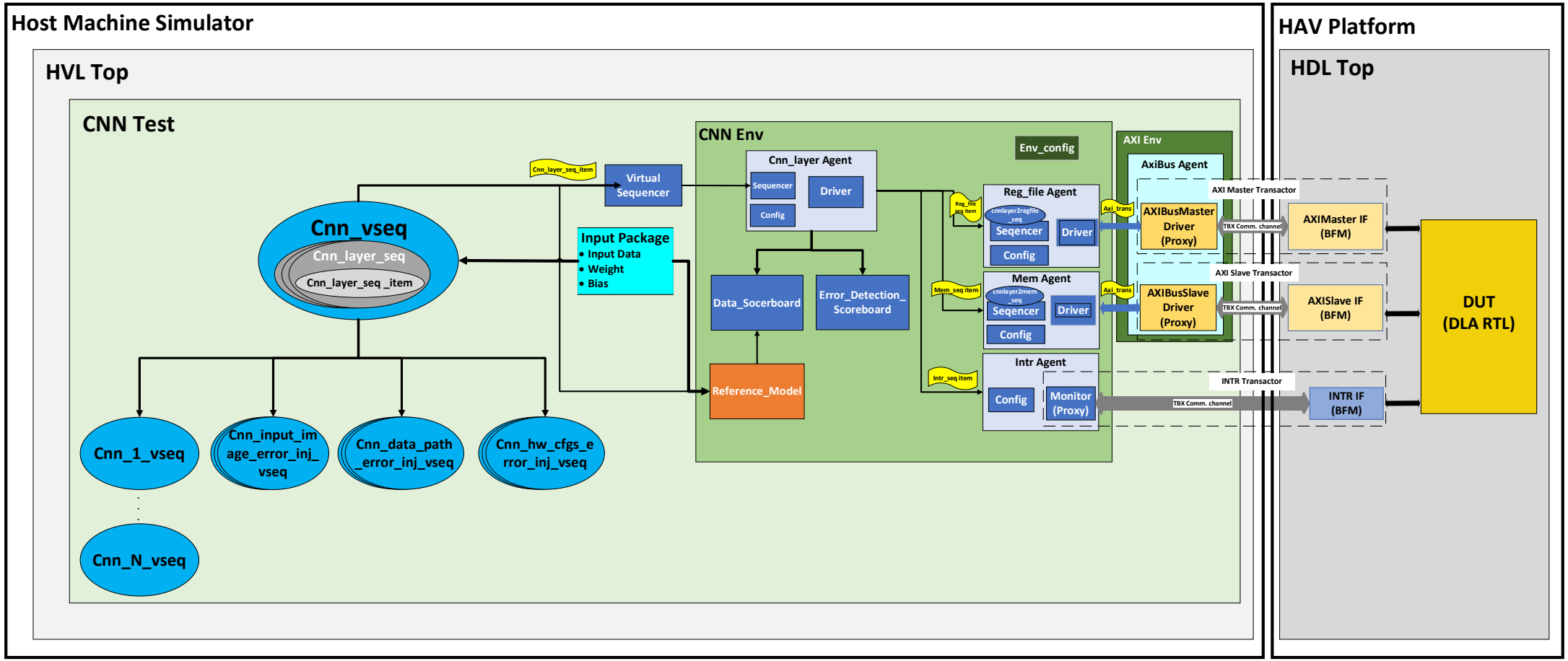
UVM Testbench Architecture



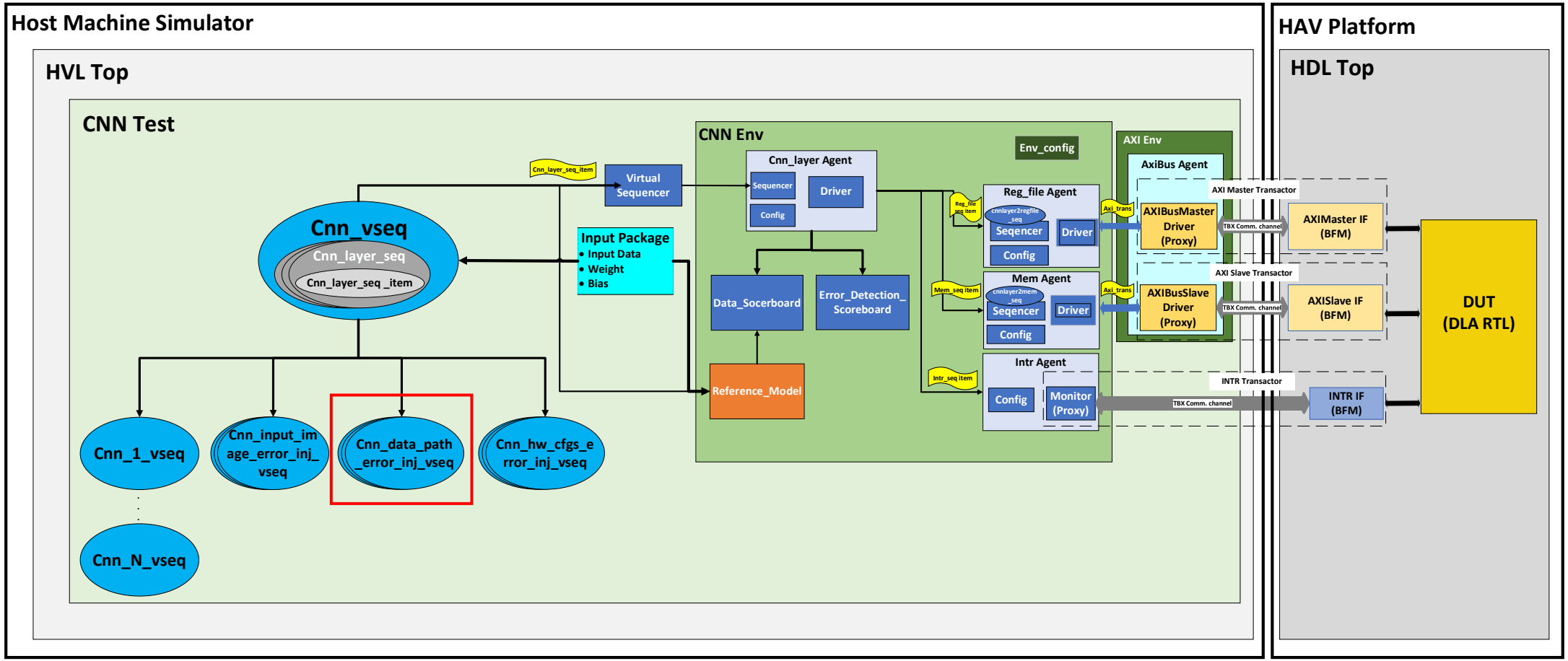
Timed HDL and Untimed HVL Partitioning



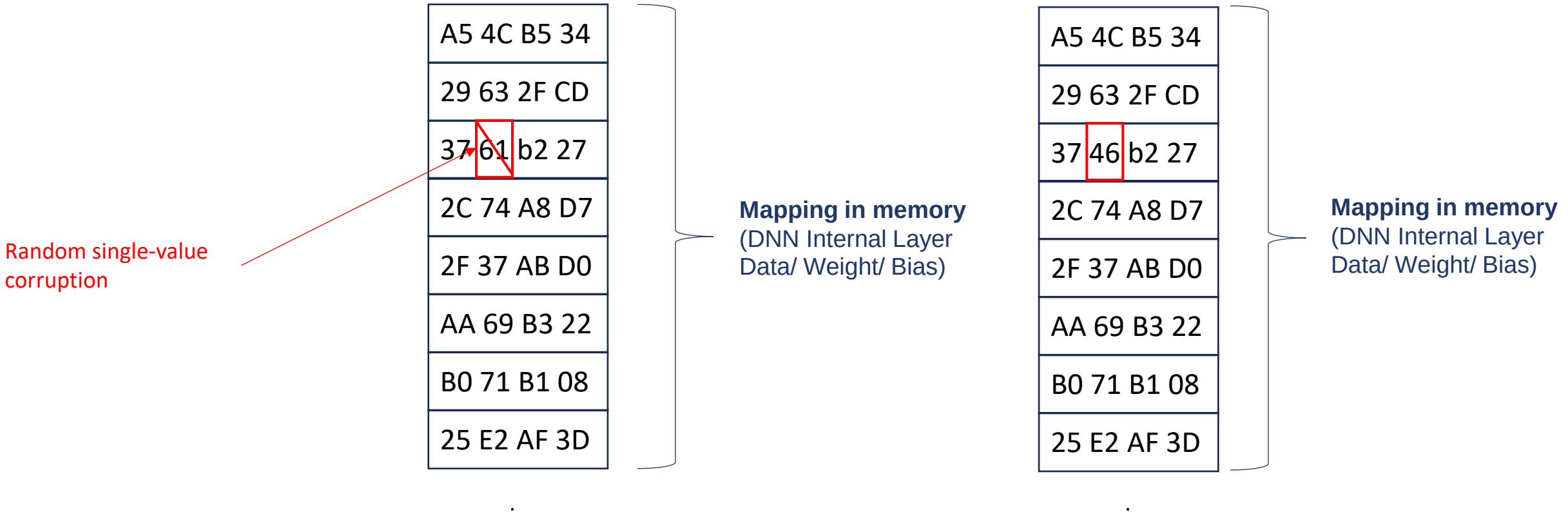
UVM Testbench Architecture



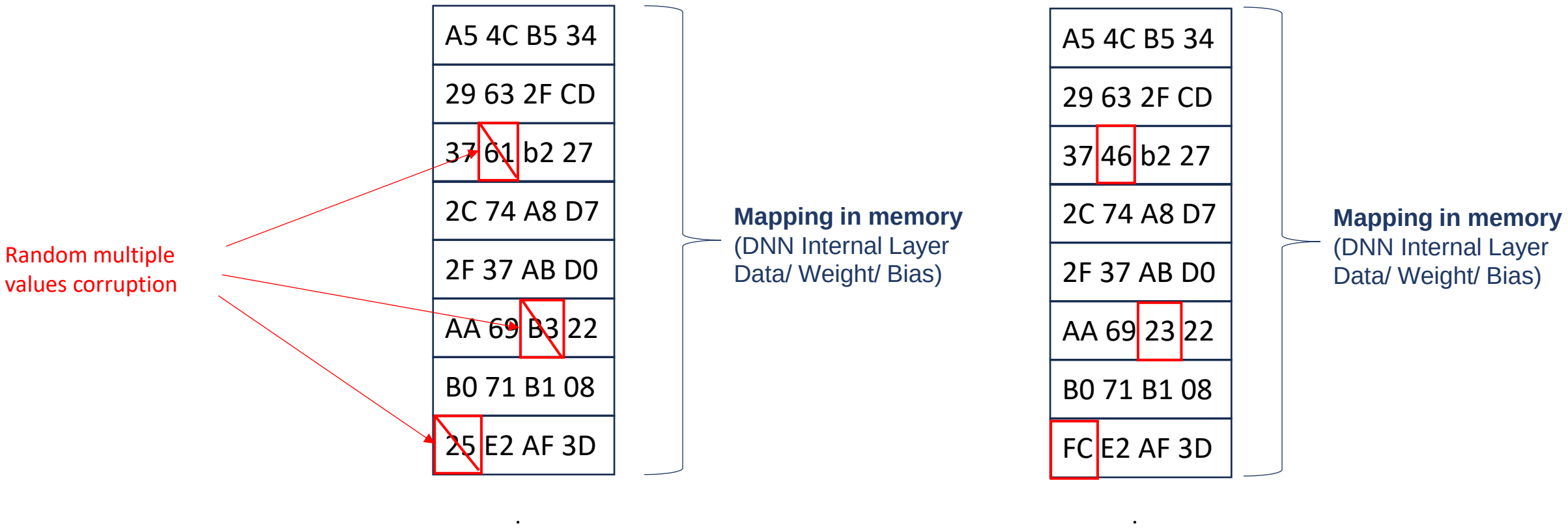
1. DNN Data Path Error Injection



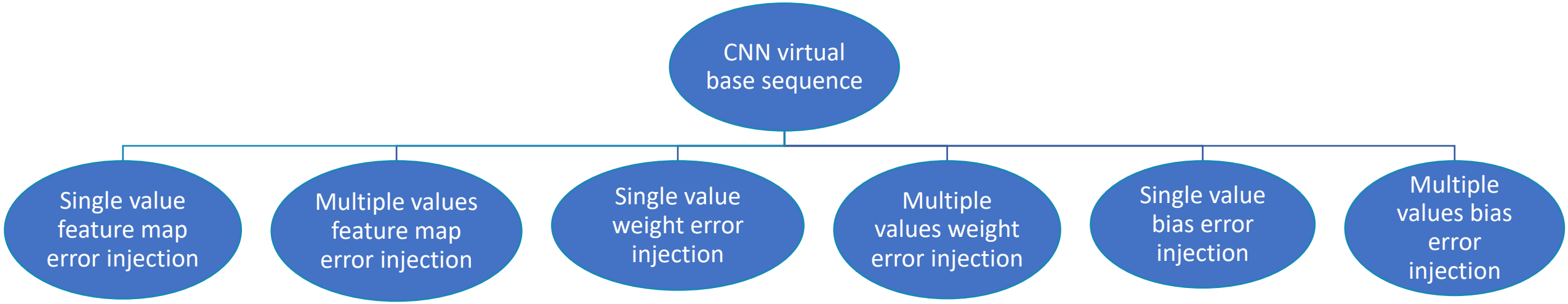
1. DNN Data Path Error Injection



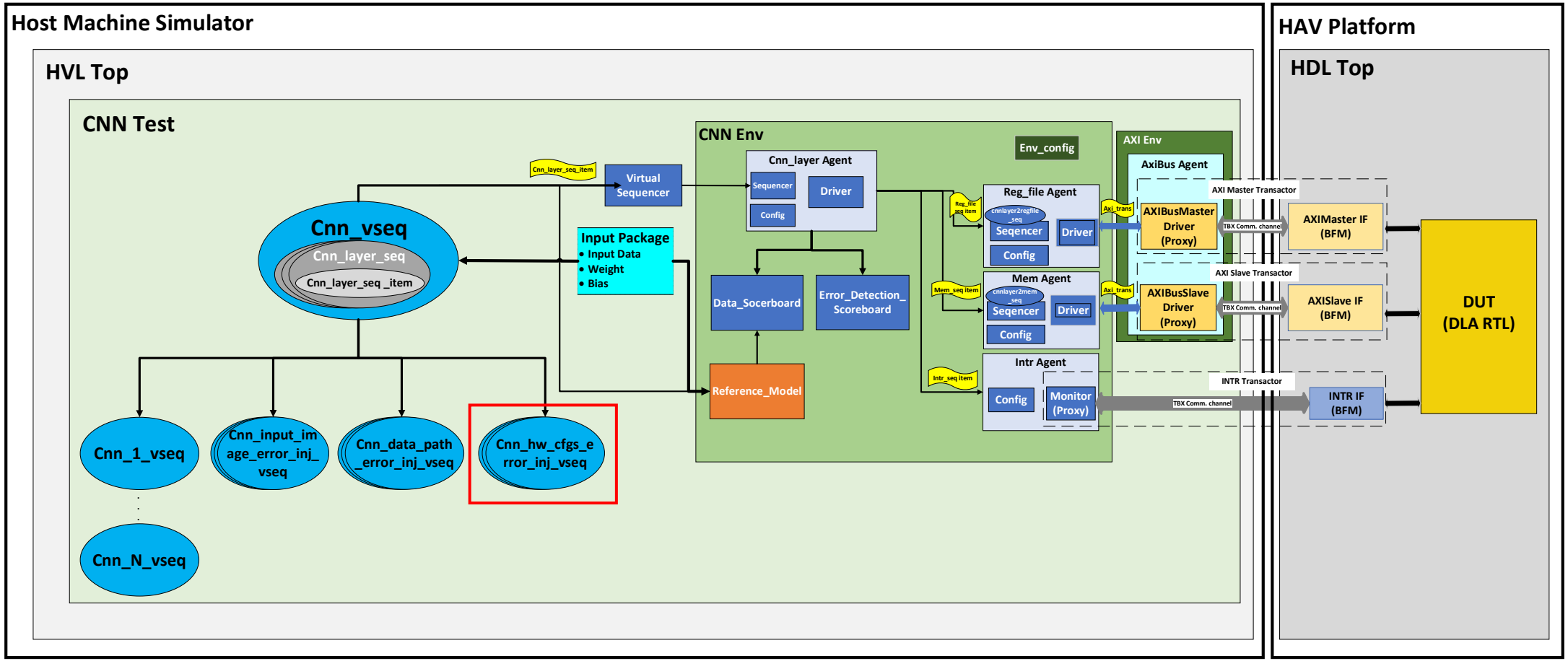
1. DNN Data Path Error Injection



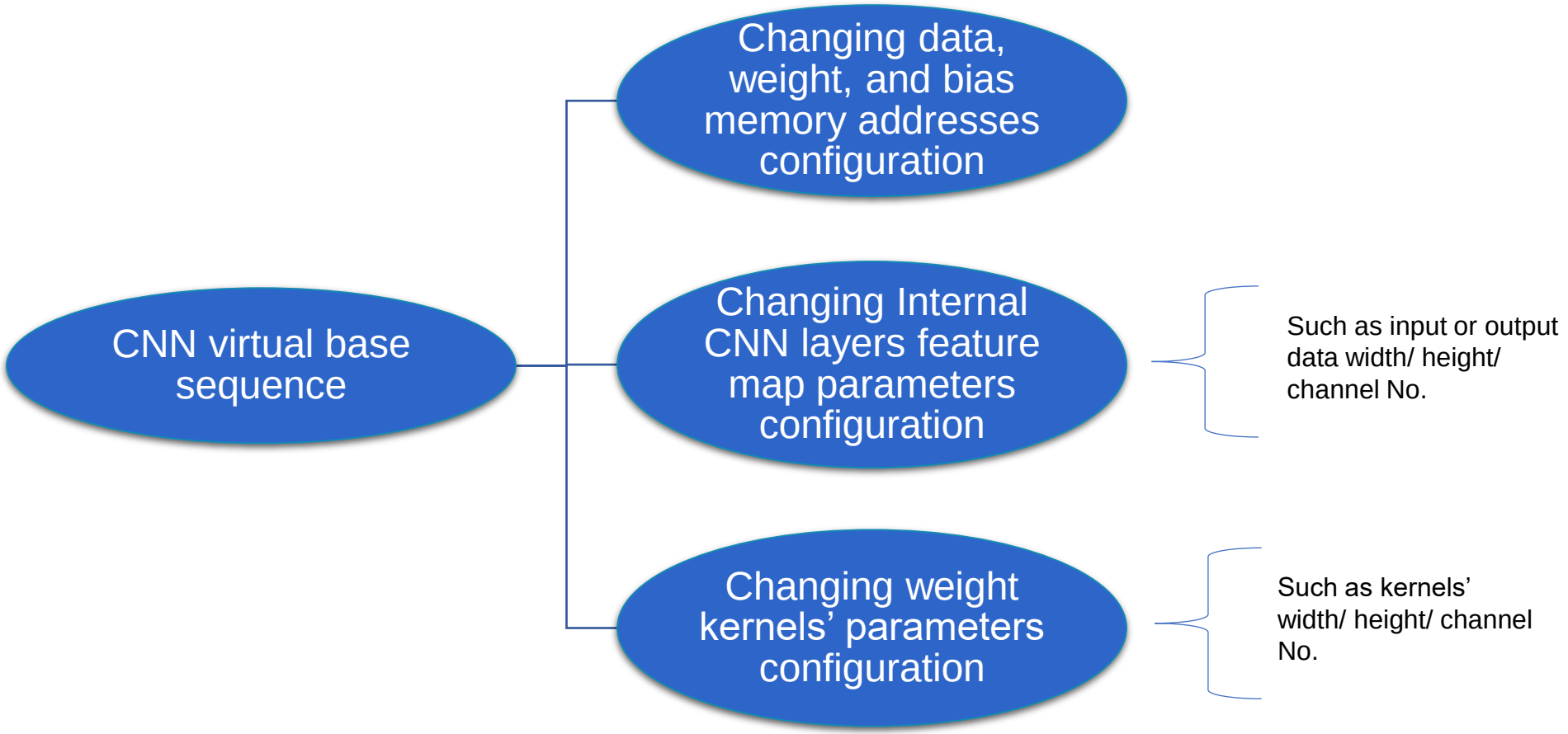
1. DNN Data Path Error Injection



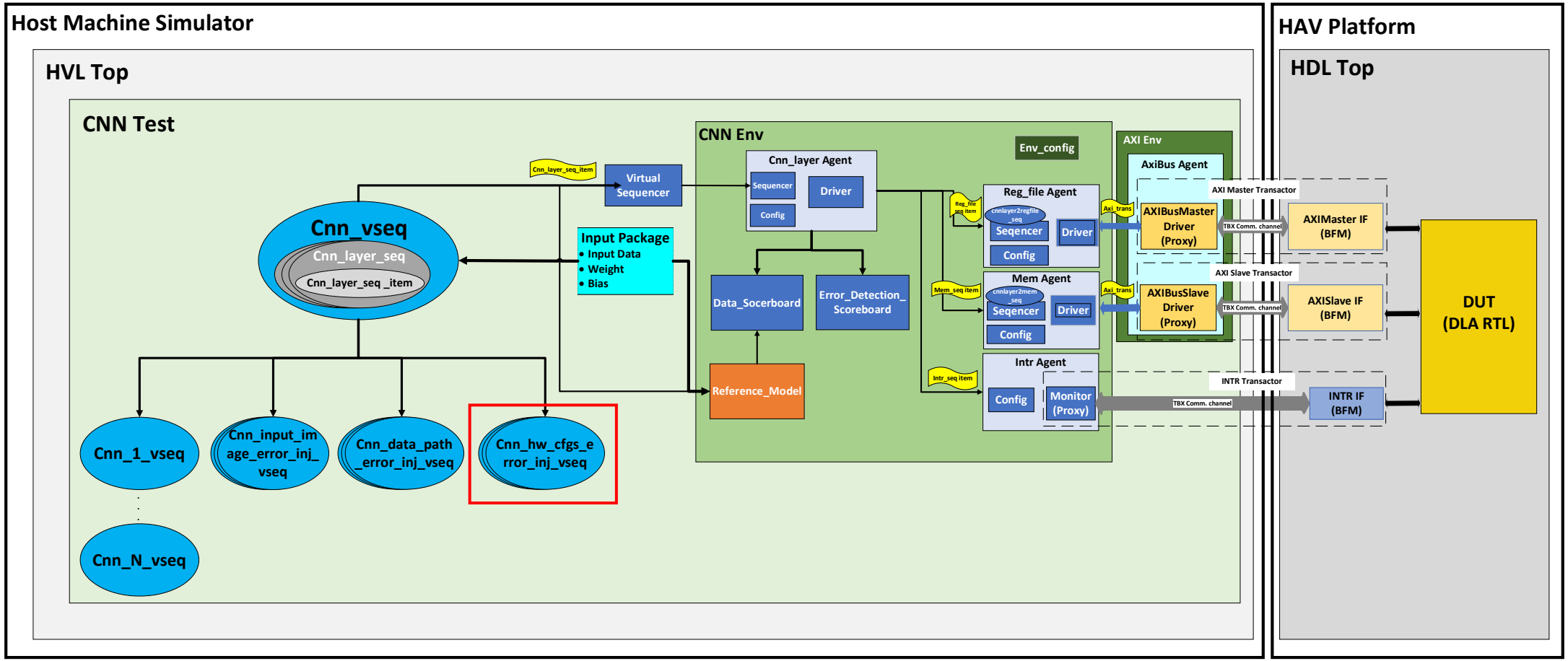
2. DLA Hardware Registers Error Injection



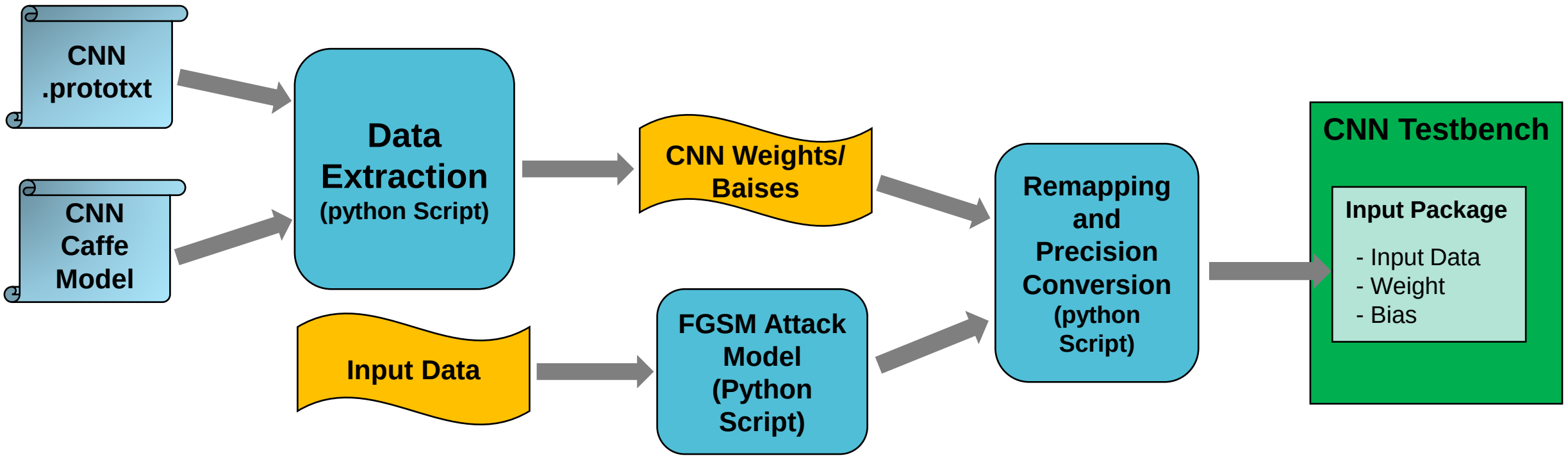
2. DLA Hardware Registers Error Injection



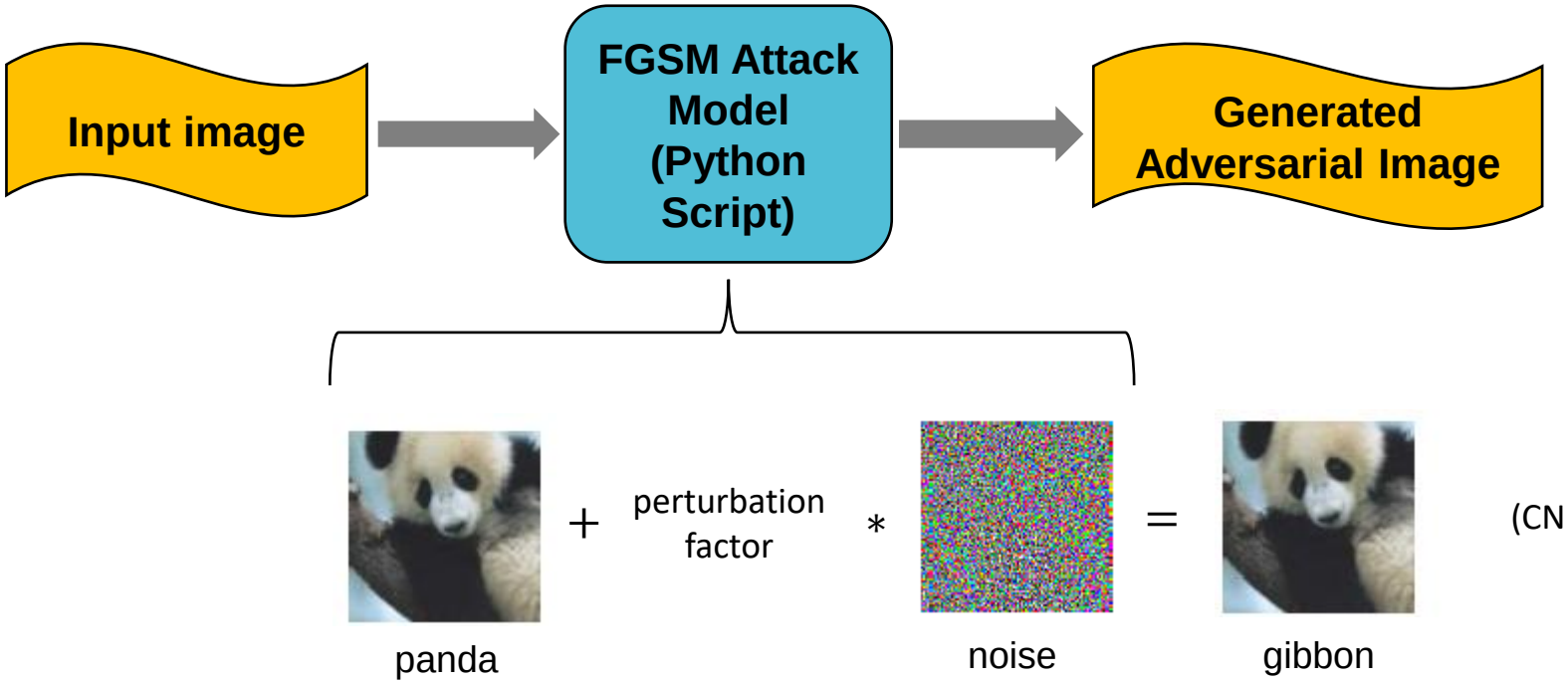
2. DLA Hardware Registers Error Injection



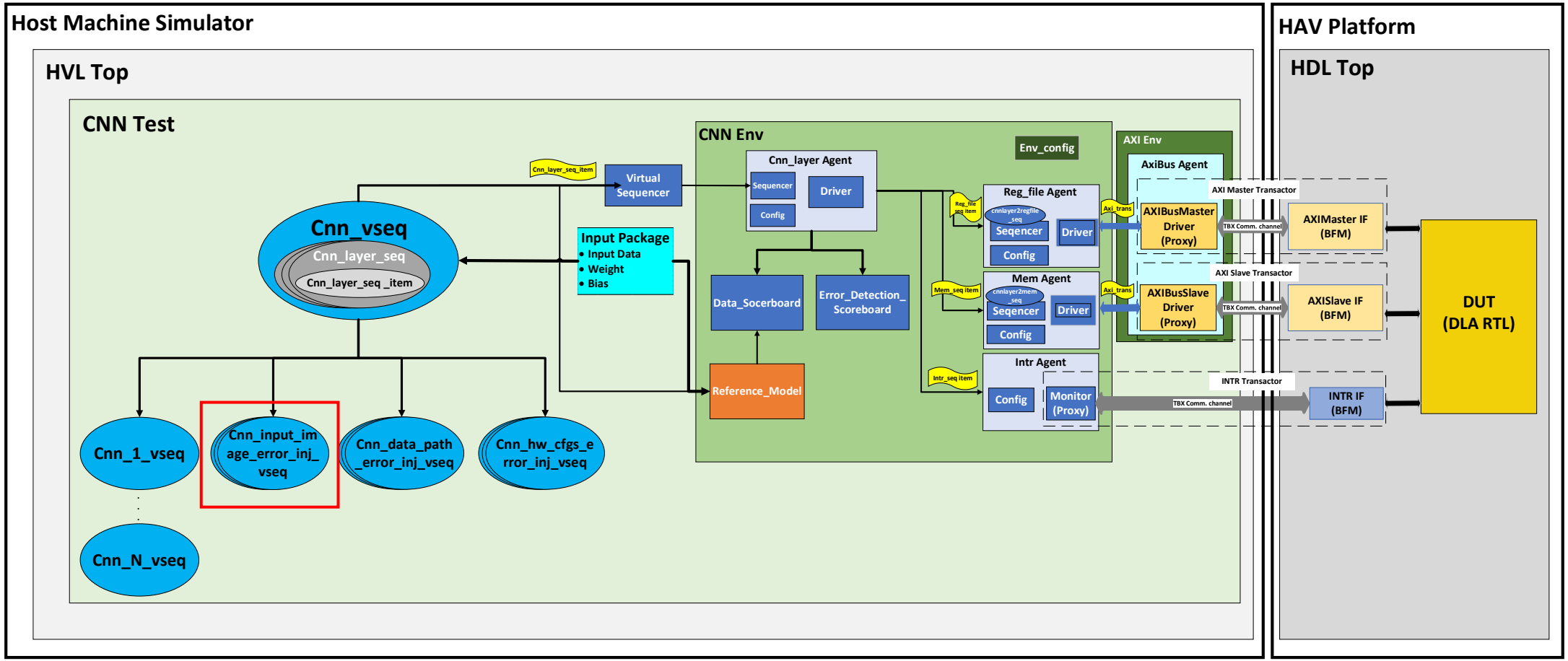
3. DNN Input Image Error Injection



3. DNN Input Image Error Injection

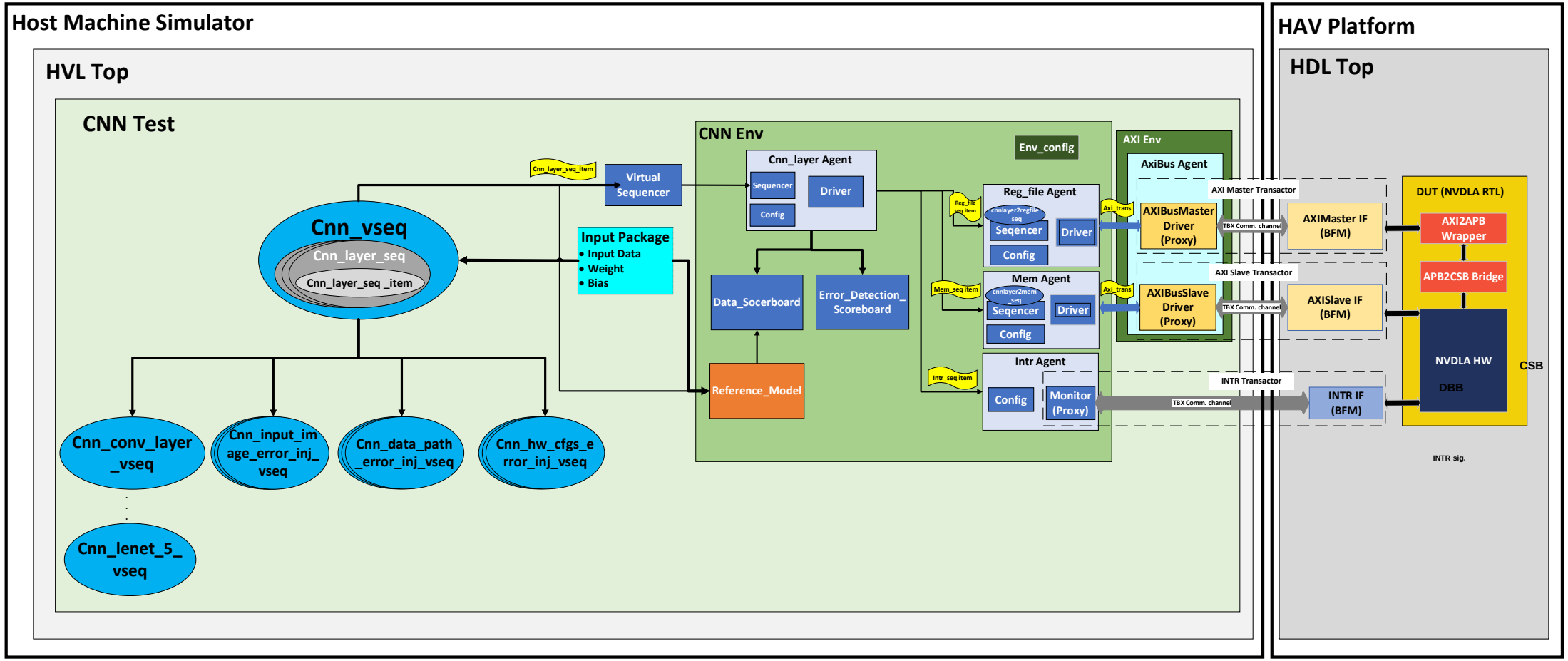


3. DNN Input Image Error Injection



NVDLA Case Study

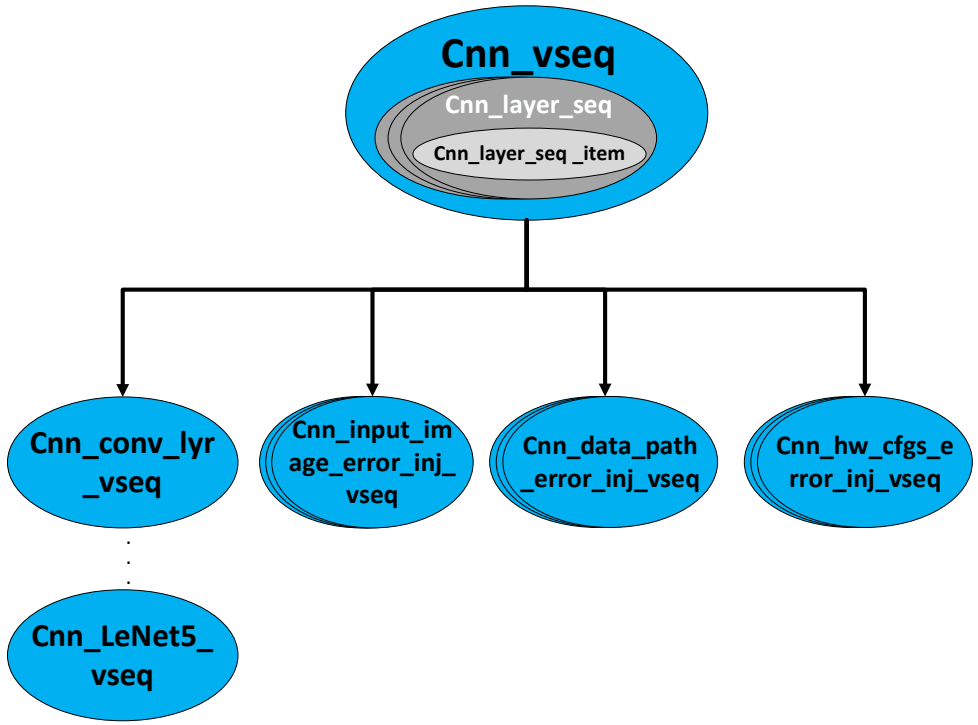
NVDLA Integration with The UVM Testbench



Experimental Results

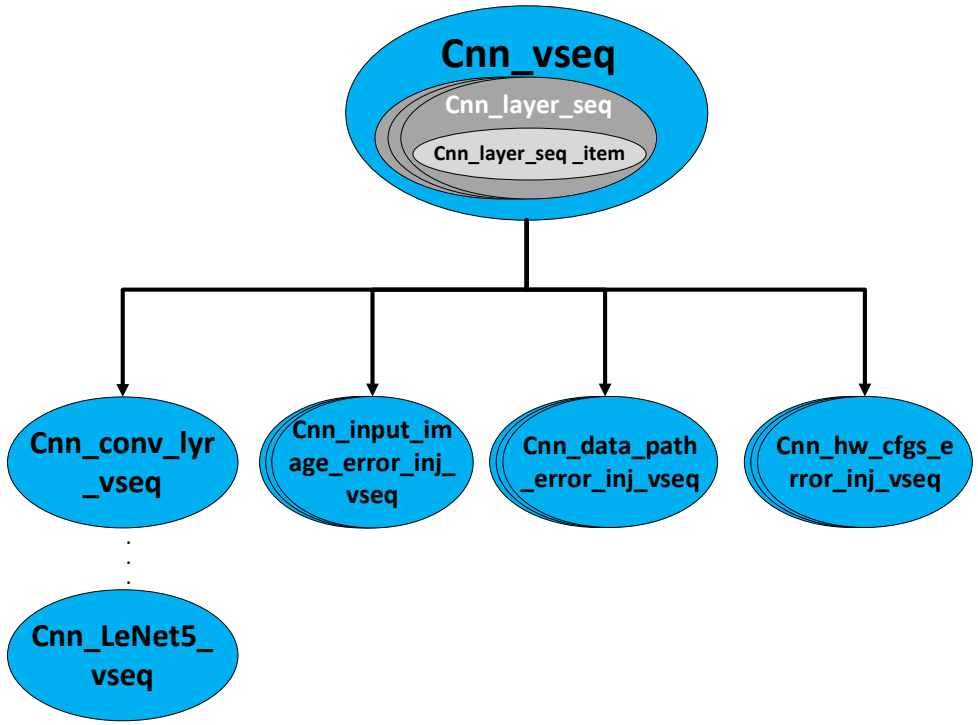
Experimental Results

- The proposed framework is used to verify the NVDLA inference function for simulation and emulation.
- Error Injection is applied to two testing scenarios as a showcase
  - Single convolutional layer
  - LeNet-5 CNN

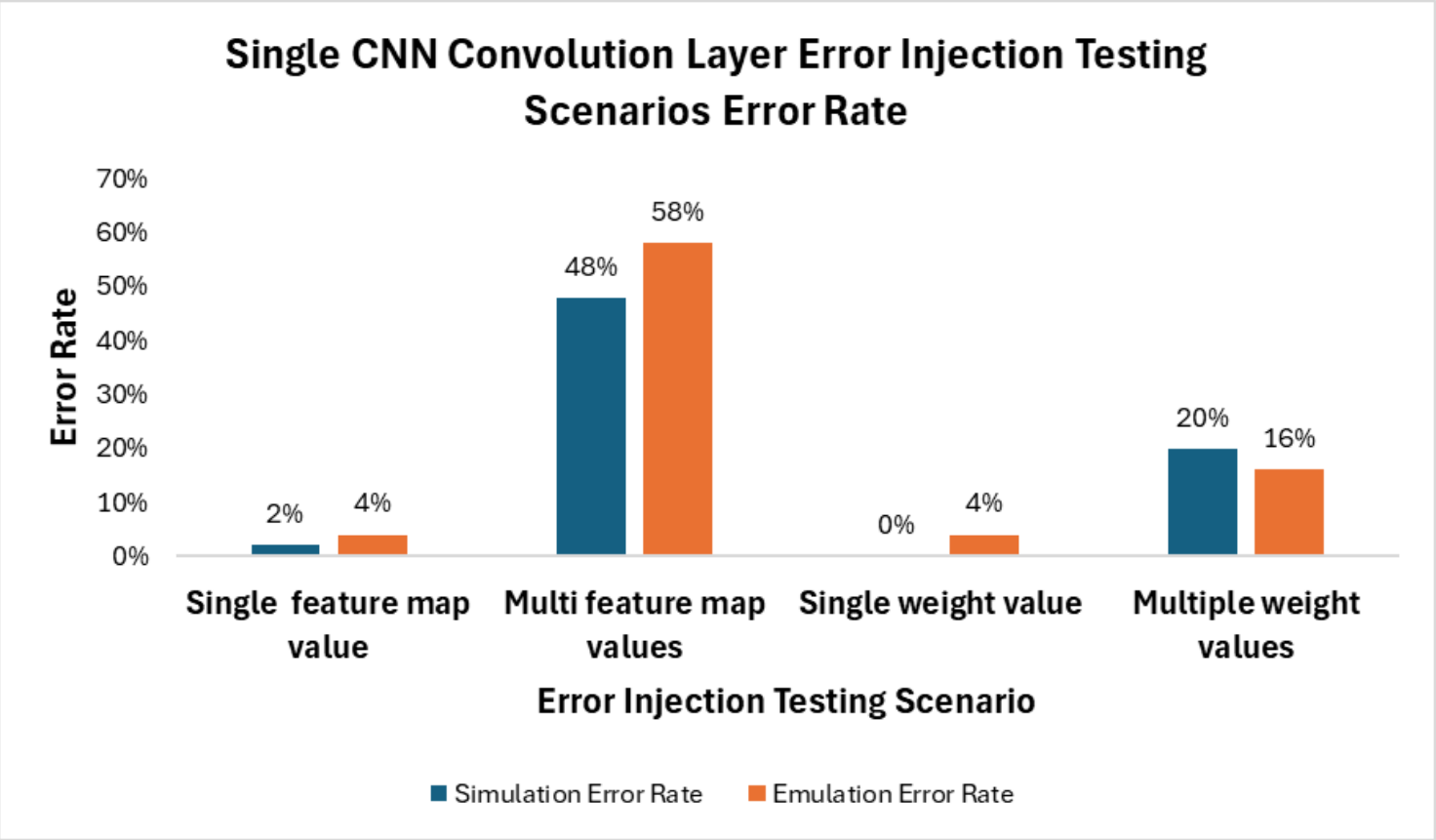


Experimental Results

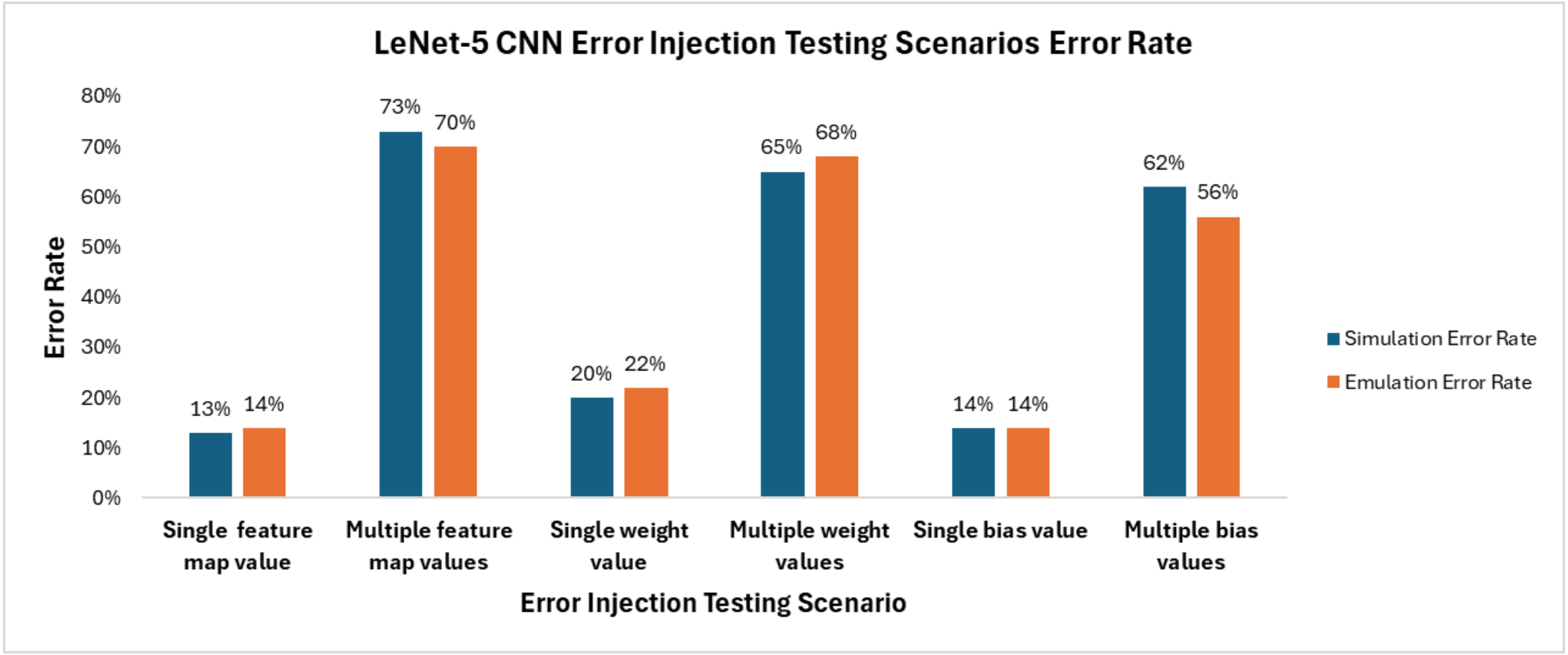
- However, The proposed framework is applicable to custom and standard CNN architectures .
- The tool used for simulation is the QuestaSim simulator.
- The platform used for emulation is Veloce Strato



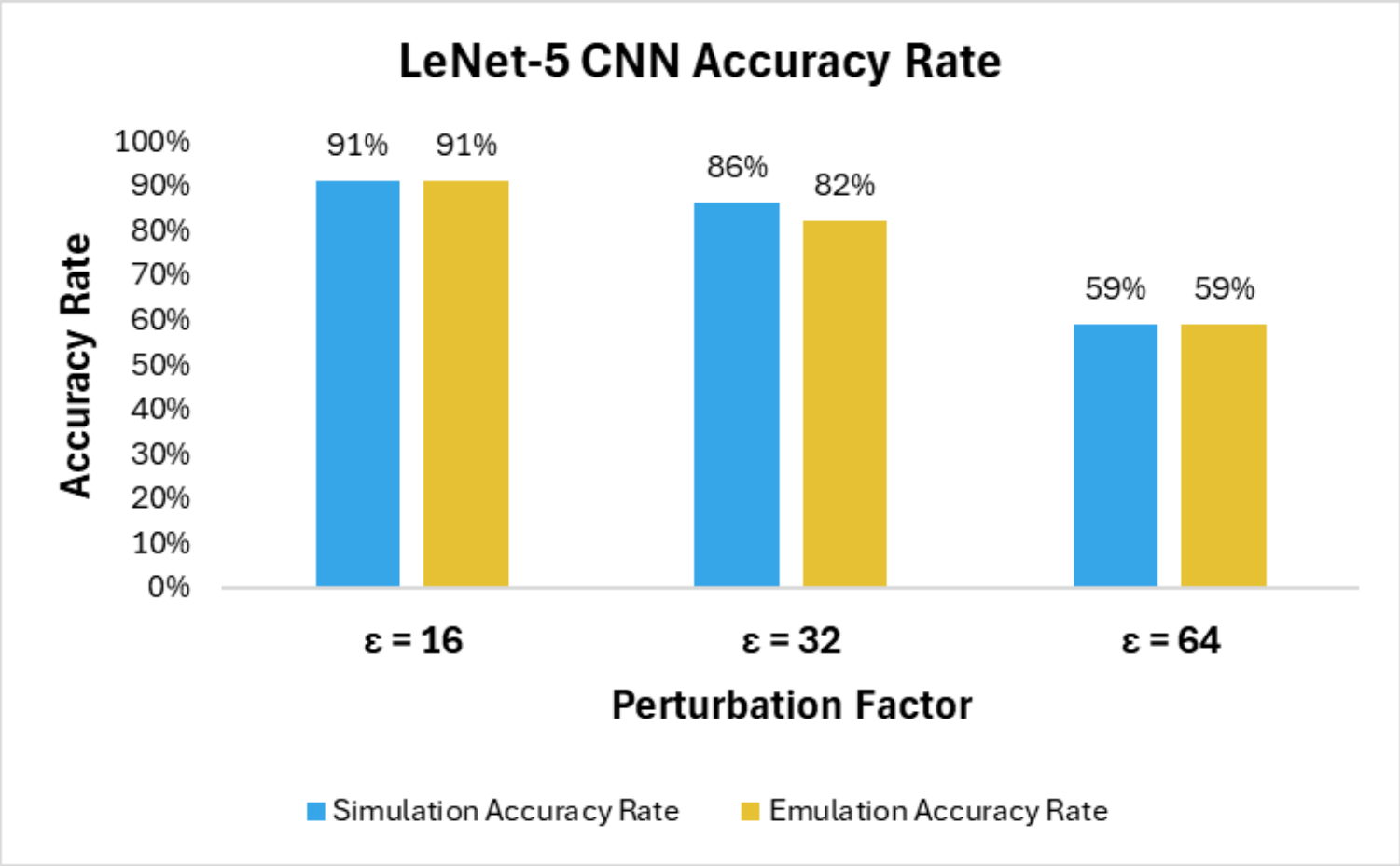
Data Path Error Injection for Single CNN Convolution Layer Results

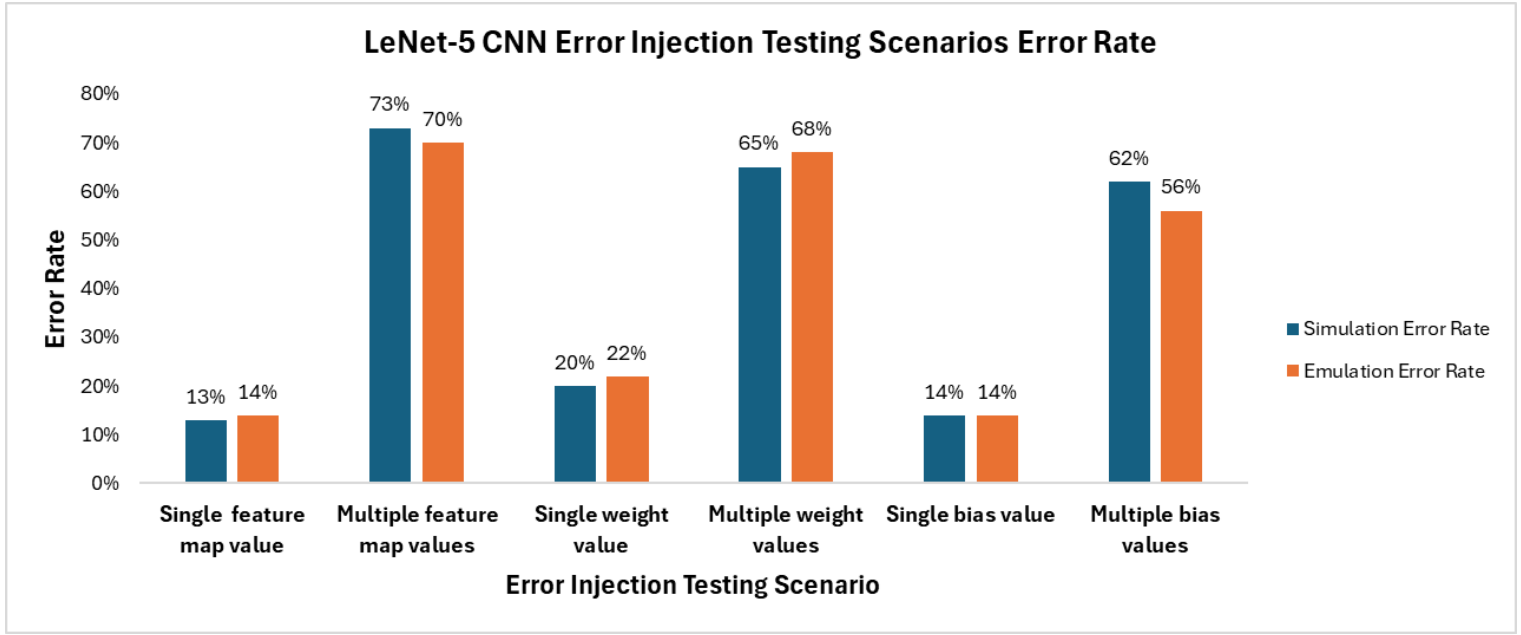


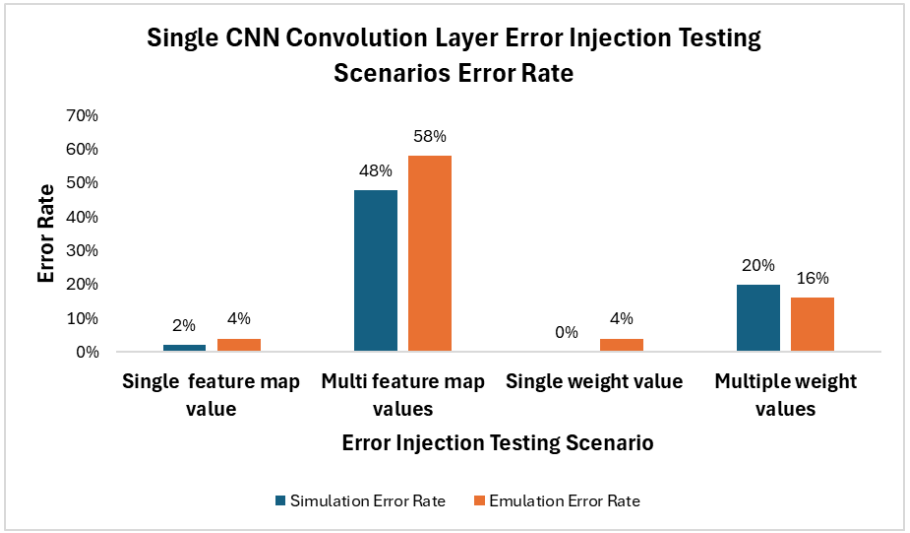
Data Path Error Injection for LeNet-5 CNN Results

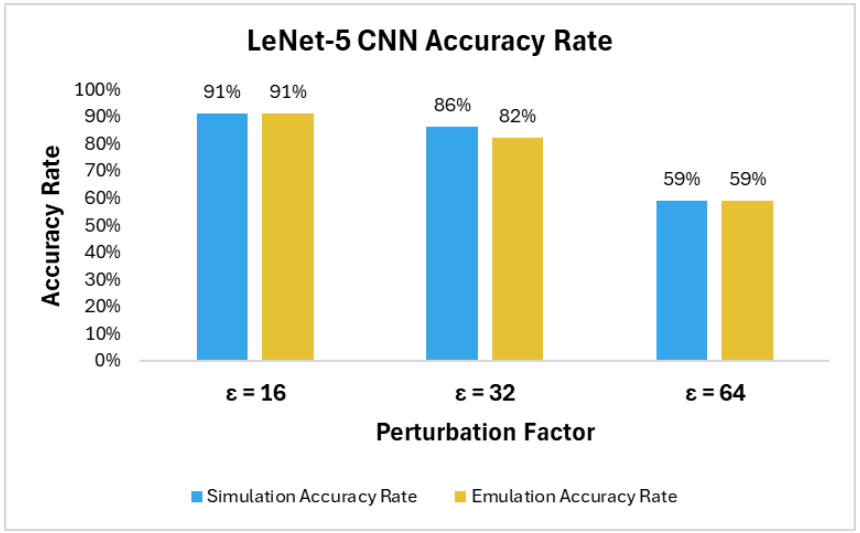


Input Image Error Injection for LeNet-5 CNN Results

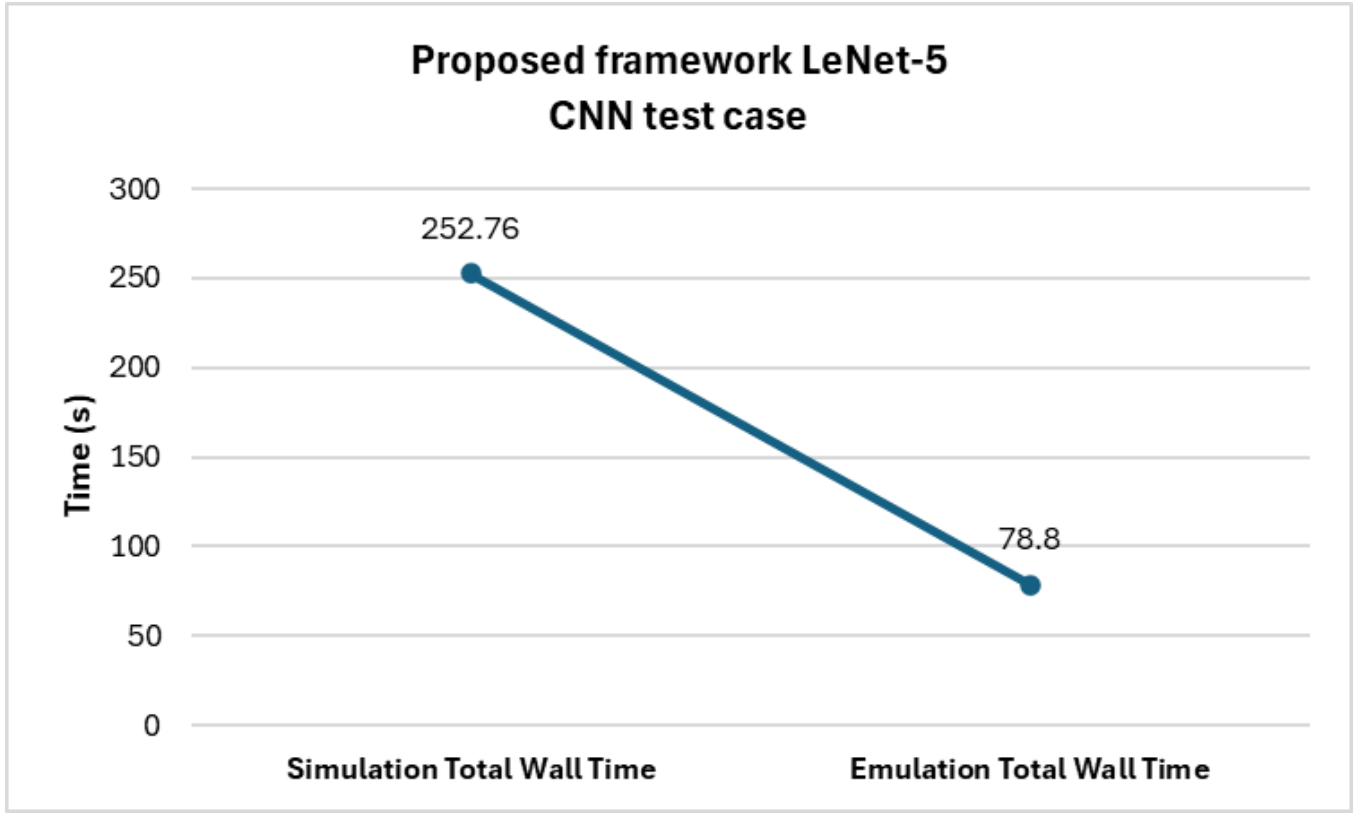



LeNet-5 CNN Error Injection Testing Scenarios Error Rate
Error Rate
80%
70%
60%
50%
40%
30%
20%
10%
0%
13%
14%
73%
70%
20%
22%
65%
68%
14%
14%
62%
56%
Single feature map value
Multiple feature map values
Single weight value
Multiple weight values
Single bias value
Multiple bias values
Error Injection Testing Scenario
Simulation Error Rate
Emulation Error Rate


Single CNN Convolution Layer Error Injection Testing Scenarios Error Rate
Error Rate
70%
60%
50%
40%
30%
20%
10%
0%
2%
4%
48%
58%
0%
4%
20%
16%
Single feature map value
Multi feature map values
Single weight value
Multiple weight values
Error Injection Testing Scenario
Simulation Error Rate
Emulation Error Rate


LeNet-5 CNN Accuracy Rate
Accuracy Rate
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
91%
91%
86%
82%
59%
59%
ε = 16
ε = 32
ε = 64
Perturbation Factor
Simulation Accuracy Rate
Emulation Accuracy Rate

Proposed framework Error Injection simulation versus emulation wall time



Conclusion

Conclusion

- The proposed error injection methodology tests the trustworthiness of complex DLA designs,
- mainly in the presence of data corruption either due to hardware faults or input perturbations.
- The proposed methodology added more flexibility and scalability with the cross-layer error injection in the DNN.
- Running the UVM testbench for emulation accelerates the verification process.
- A CNN is more sensitive to the internal layers' multiple values of input data, weight, and bias corruption compared to a single value corruption propagation between layers.

Future Work

Future Work

- Implementing testing scenarios to run other more complex CNNs with and without defense mechanisms on the NVDLA to check the system's stability and analyze the resilience of such CNNs against faults and attacks.

- Running the proposed framework on FPGA prototyping system for better performance.

Questions

Questions

Randa Aboudeif

aranda@aucegypt.edu