PADERBORN UNIVERSITY

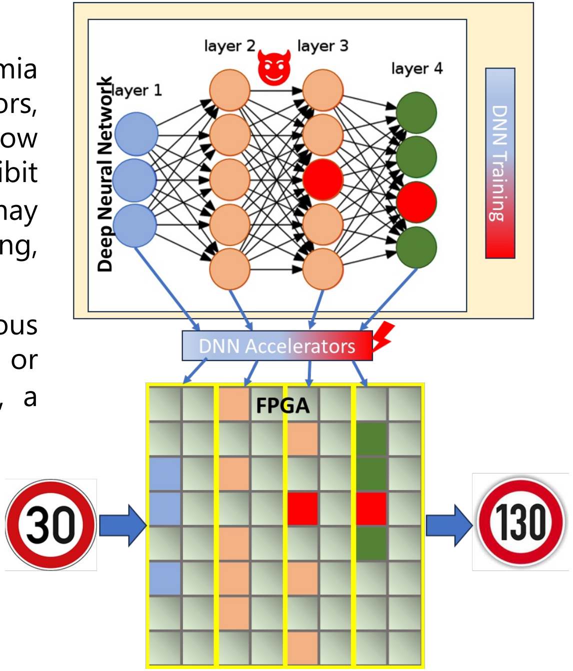
# Open Master‘s Thesis Project

Computer Science Department
Computer Engineering Group
Prof. Dr. Marco Platzner

## Hardware Trojans in Custom-tailored Dataflow Accelerators

Deep Neural Networks (DNNs) are playing a vital role to facilitate the industries and academia in application domains such as computer vision, autonomous driving, IoTs, healthcare sectors, etc. Most of the applications require a huge amount of data to be processed efficiently with low latency under real-time constraints. Custom-tailored hardware accelerators for DNNs exhibit lowest latency and are thus well-suited for such applications. However, these accelerators may prone to attacks, such as the insertion of backdoors or hardware Trojans during training, compression or deployment.

This thesis demonstrates the introduction of hardware Trojans into DNNs by malicious transformations during DNN design and deployment. The Trojans can be activated directly or by specific inputs during inference. The project uses FINN (https://finn.readthedocs.io), a popular open source framework for creating FPGA-based dataflow accelerators for DNNs.



### Type of project

- Researching existing DNN approaches for the recognition of German traffic signs
- Training and implementing backdoors / hardware Trojans in DNNs using FINN

### Prerequisites

- Basic ML and DNN knowledge
- Experience with Python, Pytorch, HDL, and Xilinx tools is helpful

**Interested?**

Please contact Dr. Qazi Ahmed, O3 137

qazi@mail.upb.de