CAREER: Enabling Trustworthy Upgrades of Machine-Learning Intensive Cyber-Physical Systems

Weiming Xiang, School of Computer and Cyber Sciences, Augusta University

https://www.nsf.gov/awardsearch/showAward?AWD_ID=2143351

Goal: Develop verification and upgrade procedures to provide **formal safety guarantees for ML-intensive CPS throughout life cycles.**

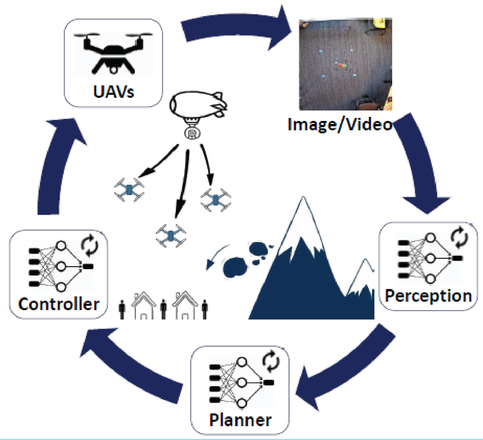
Challenges

- **Vulnerabilities of ML Components**

  How to fully identify the incompatibilities caused by the ML upgrade, and formally verify upgrades of ML-intensive CPS?

- **Unique Upgrade Procedures of ML Components**

  How to develop safety-assured ML upgrade for ML-intensive CPS?



Scientific Impacts

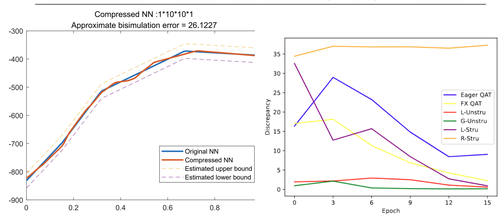
- ***Safe Upgraded Model:*** Safety Verification and Monitoring of ML-Intensive CPS Upgrades
- ***Safe Upgrade Procedure****:* Safety-Assured Upgrades for ML-Intensive CPS
- ***Safe Upgrade Application:*** Safe Upgradable ML-Intensive Autonomy

Project Progress

- Reachability-Based Verification Feedforward Neural Network (FNN) and Convolutional Neural Network (CNN) Compression
- Assured Output Restoration for FNN and CNN Compression
- Formal Equivalence Evaluation on Neural Network Compression Methods

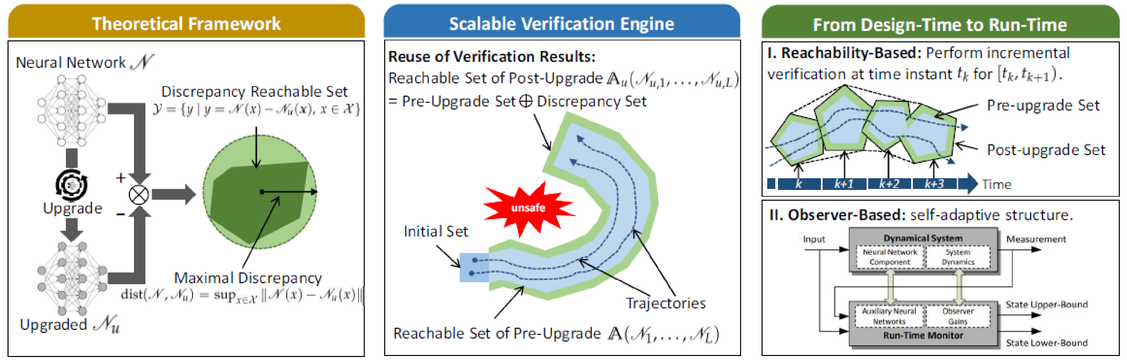
Table 1. Comparison among compression methods for CNN with MNIST dataset

Network	Parameters	Size	Sparsity	Accuracy	Discrepancy ρ^*
Original network	1.2 M	4690 KB	0%	98%	-
Eager QAT network	1.2 M	1184 KB	0%	99%	2.6147
FX QAT network	1.2 M	1179 KB	0%	99%	7.3433
Eager Static network	1.2 M	1184 KB	0%	96%	>10.0937
FX Static network	1.2 M	1179 KB	0%	94%	3.4256
L-Unstru network	1.2 M	4690 KB	20%	98%	0.6061
G-Unstru network	1.2 M	4690 KB	20%	98%	**0.0604**
L-Stru network	1.2 M	4690 KB	19.97%	98%	0.6670
R-Stru network	1.2 M	4690 KB	19.97%	97%	10.6880

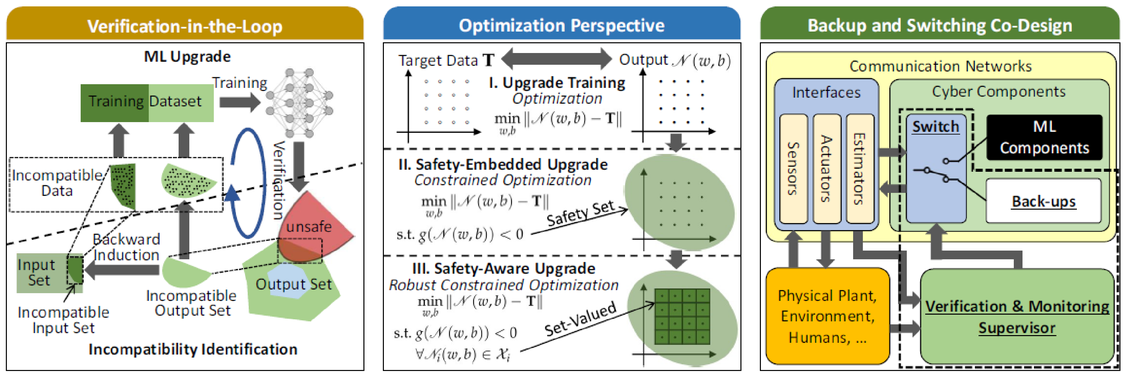


Solution

- **Safety Verification and Monitoring of ML-Intensive CPS Upgrades**



- **Safety-Assured Upgrades for ML-Intensive CPS**



Broader Impacts

Impact to Society

- The techniques and tools will benefit CPS and ML applications to provide lifetime safety assurance.

Education and Outreach

- CPS workforce training and education, one student won DoD scholarship.
- Develop a new CPS course at AU.
- Engage in K-12 outreach activities, GenCyber Camp, High School Spotlight Event, etc.

2024 NSF Cyber-Physical Systems Principal Investigators' Meeting
March 20-21, 2024

AI-CPS Lab:
aicpslab.com

Award ID#: 2143351