Politecnico di Torino

# COMPUTER AND CONTROL ENGINEERING

## DAUIN - Cybersecurity and Reliability of Automotive Embedded Systems leveraging ML algorithms in the V2X Era

| | |
|---|---|
| **Funded By** | Dipartimento DAUIN |

| | |
|---|---|
| **Supervisor** | SANCHEZ SANCHEZ EDGAR ERNESTO - ernesto.sanchez@polito.it |

| | |
|---|---|
| **Contact** | SAVINO ALESSANDRO - alessandro.savino@polito.it<br>RUOSPO ANNACHIARA - annachiara.ruospo@polito.it<br>DI CARLO STEFANO - stefano.dicarlo@polito.it |

| | |
|---|---|
| **Context of the research activity** | The growing use of machine learning and V2X communication in automotive embedded systems enables intelligent and connected vehicles but introduces new cybersecurity and reliability risks. ML components face threats such as adversarial attacks, data poisoning, and faults, while V2X expands the attack surface. This PhD proposes combining ML techniques with hardware-based security to improve both system security and ML reliability in safety-critical automotive environments. |

| | |
|---|---|
| | Current automotive cybersecurity solutions typically address either system security or functional safety in isolation, while ML reliability is often treated as a secondary concern. ML-based security mechanisms, such as intrusion detection systems, are vulnerable to adversarial attacks and data integrity issues. Conversely, hardware security mechanisms provide static protection but lack adaptive capabilities to detect and respond to evolving threats or ML failures.<br>Prior research has demonstrated vulnerabilities in automotive embedded systems and V2X communication, including message injection, spoofing, and denial-of-service attacks. ML-based intrusion detection systems have shown improved detection capabilities, but they are susceptible to adversarial examples, data poisoning, and performance degradation due to concept drift.<br>Research on ML reliability and trustworthiness has highlighted challenges such as explainability, robustness, and fault tolerance, particularly in safety-critical systems. Hardware security research provides strong guarantees for secure boot, cryptographic operations, and system integrity but has limited focus on protecting ML workflows. Existing studies rarely address the co-design of ML reliability and hardware security in automotive V2X environments, which this research aims to fill. Actually, there is a critical need for integrated security architectures that jointly address cybersecurity threats and ML reliability in connected automotive embedded systems. For these |

**Objectives**

reasons, this research proposal intends to investigate the following topics:
- Ensuring the reliability and trustworthiness of ML models deployed on resource-constrained automotive embedded systems
- Protecting ML models and training/inference data against cyberattacks in V2X environments
- Detecting ML misbehavior caused by adversarial inputs, data drift, or hardware faults
- Integrating hardware-enforced trust with adaptive ML-based security under real-time constraints

Main research goal:
To design, implement, and validate an integrated framework that leverages machine learning and hardware-based security to enhance the cybersecurity and reliability of ML-enabled automotive embedded systems operating in the V2X era.

Proposal objectives

- To analyze the interaction between ML components, embedded automotive architectures, and V2X communication systems
- To identify cybersecurity threats and reliability risks affecting ML-enabled automotive embedded systems
- To develop lightweight ML-based mechanisms for attack detection and ML behavior monitoring
- To leverage hardware security features to ensure model integrity, data authenticity, and trusted ML execution
- To experimentally validate the proposed framework under realistic cases of study

Methodology
1 System reliability and Threat Analysis
- Study of ML-enabled automotive embedded architectures and V2X stacks
- Threat and risk modeling covering cybersecurity and ML reliability aspects
- Identification of attack and failure scenarios affecting ML applications

2 ML Reliability and Security Mechanisms
- Design of lightweight ML models for anomaly detection and behavior monitoring
- Development of techniques for detecting data drift, adversarial inputs, and model degradation
- Development of techniques for detecting hardware reliability issues

3 Hardware-Based Trust and Protection
- Use of HSMs or secure enclaves for trusted ML inference and key management
- Hardware-enforced integrity checks for ML models and data
- Device authentication and binding of ML models using hardware solutions

4 Experimental Validation
- Simulation of V2X scenarios using established vehicular network simulators
- Prototyping on automotive-grade embedded platforms
- Evaluation metrics: detection accuracy, reliability, latency, resource

| | |
|---|---|
| | overhead, and safety impact<br><br>The expected contributions of this Ph.D. proposal are:<br>- A novel integrated framework for cybersecurity and ML reliability analysis in automotive embedded systems<br>- Methods for runtime monitoring and protection of ML models in V2X environments<br>- Hardware-assisted techniques to enhance trust and robustness of ML-based security mechanisms<br><br>the Ph.D. project is expected to be developed following these phases:<br>Year 1:<br>Literature review, system analysis, threat modeling, definition of ML reliability metrics, definition of some relevant cases of study covering security and reliability aspects<br><br>Year 2:<br>Design and implementation of ML and hardware-based security mechanisms supported on the previously defined cases of study<br><br>Year 3:<br>Experimental validation, verification and testing of the previously defined scenarios<br><br>The candidate is expected to publish in high-impact journals (e.g., IEEE TCAD, IEEE TOC, IEEE Vehicular Technology Magazine, IEEE D&T) and present findings at leading conferences (IEEE DATE, HOST, IEEE VTC, IEEE ETS, IEEE ITC, USENIX). |

| | |
|---|---|
| **Skills and competencies for the development of the activity** | Mandatory Skills:<br>- Proficiency in Python, PyTorch, CUDA, and HPC workflows<br>- Good background in machine learning, deep learning and AI modeling<br>- Good background in hardware security<br><br>Preferred Skills<br>- Computer design and architectures<br>- RISC-V ISA. |