Politecnico di Torino
Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering
XXXVI cycle

Electronic CAD & Reliability Group

Supervisor
Prof. Stefano Di Carlo
Prof. Ernesto Sanchez

Cybersecurity applied to embedded control systems

PhD Candidate: *Franco Oberti*

1. Introduction

The automobile industry no longer relies on pure mechanical systems; instead, it benefits from advanced Electronic Control Units (ECUs) to provide new and complex functionalities in the effort to move toward fully connected cars. However, connected cars provide a dangerous playground for hackers.

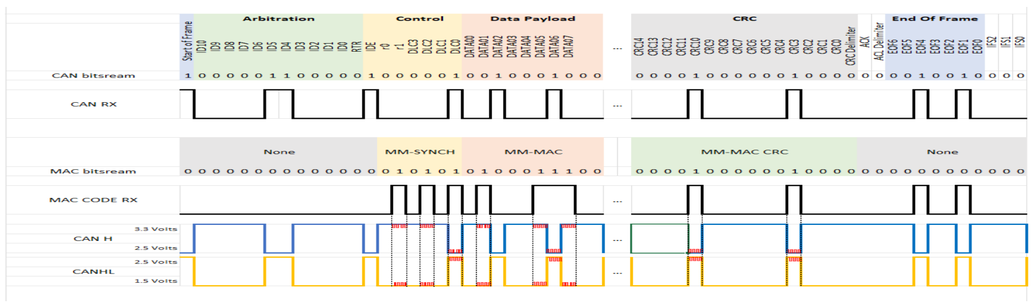
2. Goal

Exploring new approaches in the field of Product Security applied to Road Vehicles able to assure a sufficient level of resiliency to cyber attacks for the entire lifecycle as per legislation obligations.

3. Trust architecture and technique for vehicle communications

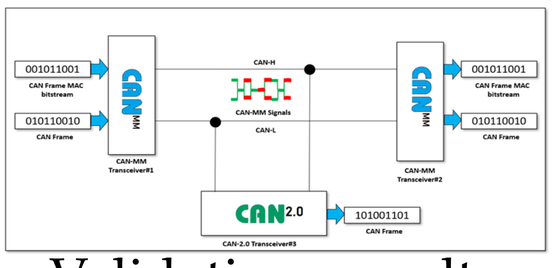
The starting point for the research activities is a crucial asset in road vehicles, COMMUNICATION.

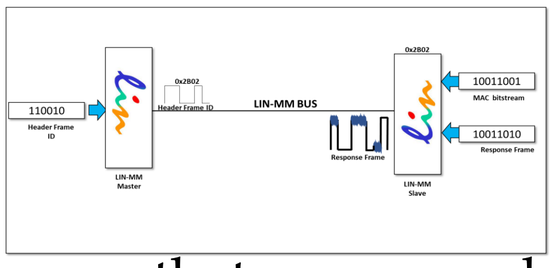
- **EXT-TAURUM P2T** [1]: authentication of hardware modules connected through Controller Area Networks (CAN) in modern vehicles is becoming an increasing security issue. Even computational time for cryptography limits the security mechanisms in safety-critical hard real-time devices. The EXT-TAURUM P2T is a new low-cost, secure CAN-FD architecture for the automotive domain, implementing a novel key provisioning strategy, intelligent throughout management, and hardware signature mechanisms.
- **MAC MULTIPLEXED (MM)** [2] technology is an innovative method for extending the protocol payload ability in a no intrusive way, ensuring back compatibility with today's standard protocols and devices. Through digital signal modulation techniques, it is possible to multiplex the MAC bit stream on the physical, electrical signal of the communication frame to protect both the CAN network and LIN networks from some specific attacks. Especially, it is very resilient to Spoofing Attacks, Man in the Middle (MitM) and Tamper Attacks.



4. Results

The MM technology has been validated with SPICE models while TAURUM P2T through a minimal open loop test bench.





Validation results prove that our novel solutions make vehicle networks more secure, keeping the back compatibility with today's architecture. So far, the MM is the only method for making the LIN domain secure, while CAN-MM improves MAC propagation latency time, getting crucial benefits for the system's throughput.

5. References

1. F. Oberti, A. Savino, E. Sanchez, F. Parisi and S. Di Carlo, "EXT-TAURUM P2T: An Extended Secure CAN-FD Architecture for Road Vehicles," in *IEEE Transactions on Device and Materials Reliability*,
2. F. Oberti, E. Sanchez, A. Savino, F. Parisi, M. Brero and S. D. Carlo, "LIN-MM: Multiplexed Message Authentication Code for Local Interconnect Network message authentication in road vehicles," 2022 IEEE 28th International Symposium