講演番号 196

Beyond Four Wheels: UN Regulation No. 155 Implementation in Light Mobility Vehicle Cybersecurity

Carlos Lujan [1)] **Oriol Flix** [1)] **Nadia Martínez** [1)]

1)APPLUS IDIADA

ABSTRACT: UN Regulation No.155 represents a pivotal advancement in automotive cybersecurity, establishing mandatory vehicle protection frameworks. This paper analyzes its adaptation to light mobility vehicles—motorcycles, tricycles, and quadricycles—undergoing rapid digital transformation through connectivity and assistance systems.

Light vehicles face unique cybersecurity challenges: limited computational resources, space constraints, and distinct threat vectors from exposed rider interfaces. Manufacturer CSMS implementations vary significantly, particularly in threat assessments for handlebar displays, navigation systems, and vehicle-to-vehicle communications.

Research examines regulatory evolution, manufacturer compliance strategies, and certification adaptations. Findings highlight the regulation's flexibility while identifying needs for vehicle-specific guidance in updates and supply chain management.

KEY WORDS:**UN R155, Cybersecurity, Light Mobility**

1.INTRODUCTION

While the initial focus of R155 was on securing modern passenger cars and commercial vehiceles the industry now faces a second wave of challenges. As of 2026, the sector is addressing the legacy electronic architectures and the administrative difficulty of aligning agile software development with rigid regulatory audits. More critically, the recent extension of the regulation to L-category vehicles and the complex certification requirements for multistage manufacturers (bodybuilders) have exposed a maturity gap. Unlike major automotive giants, these smaller-scale manufacturers often lack the specialized resources to navigate the requirements to prove cybersecurity compliance.

2.CYBERSECURITY FRAMEWORK

In an era where vehicles are becoming increasingly connected and autonomous, the integration of robust cybersecurity measures is paramount to ensure the safety, security, and integrity of automotive systems. As vehicles evolve into sophisticated digital platforms, the regulatory landscape governing their cybersecurity undergoes parallel transformation. This paper aims to present the regulations and legislations that define the contours of vehicle cybersecurity, examining the most influential standards shaping the global automotive industry.

Among the most significant frameworks, there are standards such as ISO/SAE 21434, UN Regulation 155, and theguidelines established by national bodies like the National Highway Traffic Safety Administration (NHTSA). Each regulatory instrument contributes a distinct perspective to the overarching goal of creating a secure ecosystem forintelligent connected vehicles. By dissecting these regulations across different jurisdictions, we seek to understand the synergies and divergences that shape the landscape of vehicle cybersecurity on a global scale.

3.CONCLUSION

Five years after the implementation of UN Regulation No. 155, the automotive industry has successfully established a global baseline for cybersecurity. However, the journey has revealed that a Cyber Security Management System (CSMS) is not a static "checkpoint" but a dynamic, lifelong commitment.

R155's holistic, non-prescriptive nature is simultaneously its greatest strength and its most significant implementation challenge. The regulation correctly recognizes that cybersecurity threats evolve continuously and therefore avoids rigid technical mandates. However, this flexibility places enormous interpretive burdens on smaller manufacturers who lack the legal and technical resources of major OEMs.

Moving forward, three critical actions are necessary:

- Enhanced supply chain Collaboration: industry-wide initiatives must close the visibility gap between OEMs and lower-tier suppliers, potentially through standardized security frameworks or shared audit resources.
- Scalable compliance models: regulatory authorities shall adapt and develop proportionate compliance pathways that recognize the distinct operational realities of different vehicle segments and manufacturing scales, without compromising core security objectives.
- Multistage harmonization protocols: greater standardization is needed in the handover of cybersecurity responsibilities between base manufacturers and specialized bodybuilders, including clear documentation requirements and liability frameworks. Interface agreements between both parties shall ensure that the cybersecurity is covered within the whole lifecycle with clear responsibilities.