



PRODUCT CYBERSECURITY POLICY

MTA S.p.A designing and manufacturing electrical and electronic products for vehicles (cars, motorcycles, trucks) and special vehicles (agricultural and earthmoving machines), acknowledges that road vehicle cybersecurity risks are an integral part of its corporate strategy.

Modern vehicle products rely on connectivity and advanced electronic capabilities that expose them to cyber threats. MTA therefore recognizes that its products must be safe, reliable and resilient against cyber-attacks, and that cybersecurity must be addressed throughout the entire product lifecycle.

Executive Management is committed to managing the corresponding cybersecurity risks and to establishing a Cybersecurity Management System (CSMS) based on ISO/SAE 21434:2021, in support of customer compliance with UNECE R155 and Cyber Resilience Act (Regulation (EU) 2024/2847) and applicable homologation requirements.

The approach to product cybersecurity management is based on risk, identifying and implementing actions proportionate to the risk level. The criteria for cybersecurity risk assessment and management are contained in the procedures and strategies defined by MTA.

The constant commitment of MTA S.p.A. to product cybersecurity is expressed in:

Cybersecurity governance: Establish and maintain a CSMS and organizational rules and processes that enable cybersecurity engineering across the product lifecycle, from concept through production, operation, maintenance and end of cybersecurity support;

Executive commitment and accountability: Demonstrate management commitment to product cybersecurity, assign and communicate cybersecurity responsibilities and authorities, and provide adequate resources to address cybersecurity activities;

Cybersecurity culture and awareness: Foster and maintain a strong cybersecurity culture, promoting awareness, competence and accountability at every organizational level, so that cybersecurity is embedded in processes and decision-making;

Cybersecurity risk management: Identify, assess and treat cybersecurity risks using a harmonized, risk-based approach throughout the product lifecycle, including threat analysis and risk assessment, vulnerability management and incident response;

Product lifecycle cybersecurity: Integrate cybersecurity activities into project-dependent management, product development, cybersecurity validation and verification, production, continual cybersecurity monitoring and post-development operations;

Interdisciplinary coordination: Establish communication channels between cybersecurity and related disciplines, including functional safety, quality, information security and privacy;

Supplier and supply chain involvement: Work closely with customers, suppliers and development partners to define distributed cybersecurity responsibilities, evaluate supplier capability and ensure cybersecurity requirements are met across the value chain;

Information sharing: Define the circumstances under which cybersecurity-related information may be shared, internally or externally, in compliance with contractual, legal and information security requirements;

Continuous improvement: Institute and maintain a continuous improvement process, leveraging lessons learned from projects, cybersecurity monitoring, incidents, vulnerabilities and organizational audits;

Regulatory and contractual compliance: Ensure compliance with all applicable laws, directives, reference standards and customer-specific cybersecurity requirements, and support organizational cybersecurity audits to verify effectiveness of cybersecurity processes;

The CSMS of MTA S.p.A., based on ISO/SAE 21434:2021 and supported by the quality management system certified in accordance with IATF 16949:2016 and ISO 9001:2015, is organized to enable cybersecurity engineering across the product lifecycle. Information security requirements applicable to product cybersecurity are addressed through MTA's Information Security Management System.

According to this Policy, MTA has prepared procedures, rules and operational indications useful for product cybersecurity, guaranteeing their continuous updating.

Through training, management is committed to internally promoting full awareness of product cybersecurity principles and objectives, so that they are considered at every company level.

Codogno, 1/9/2026

ing. Antonio Falchetti

Rev. 0, 01/09/2026