INDEX

1. REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	General Review	All	Ricardo Soares	08/10/2024		

2. Overview, Purpose and Scope

This cybersecurity policy establishes guidelines and procedures for ensuring the security of our automotive electrical/electronic (E/E) systems throughout their lifecycle, in compliance with ISO/SAE 21434.

It applies to all employees, contractors, and partners involved in the development, production, and maintenance of our automotive products.

3. Cybersecurity Management System (CSMS)

Leadership and Commitment

Senior management shall demonstrate leadership and commitment to cybersecurity by:

- Establishing and maintaining a cybersecurity culture
- Providing necessary resources for cybersecurity activities
- Ensuring integration of cybersecurity requirements into organizational processes

Roles and Responsibilities

- A Cybersecurity Manager shall be appointed to oversee the implementation of this policy

- Clear cybersecurity roles and responsibilities shall be defined for all relevant personnel

4. Risk Management

Threat Analysis and Risk Assessment (TARA)

- Conduct TARA for all E/E systems and components
- Identify and evaluate potential cybersecurity threats and vulnerabilities
- Assess the impact and likelihood of cybersecurity risks
- Develop and implement risk mitigation strategies

Continuous Monitoring

- Establish processes for continuous monitoring of cybersecurity risks
- Regularly update the TARA based on new threat intelligence and vulnerabilities

5. Security by Design

Concept Phase

- Integrate cybersecurity considerations into the early stages of product development
- Define cybersecurity goals and requirements for each product

Development Phase

- Implement secure coding practices and guidelines
- Conduct regular security testing and code reviews
- Ensure traceability of cybersecurity requirements throughout development

Production Phase

- Implement secure manufacturing processes to prevent tampering
- Ensure the integrity of software and firmware during production

Incident Response and Management

- Establish an incident response team and procedures
- Develop and maintain an incident response plan
- Conduct regular incident response drills and simulations

Supply Chain Security

- Assess and manage cybersecurity risks associated with suppliers and third-party components
- Establish cybersecurity requirements for suppliers and partners

Training and Awareness

- Provide regular cybersecurity training to all relevant personnel
- Conduct awareness programs to promote a cybersecurity culture

Continuous Improvement

- Regularly review and update this cybersecurity policy
- Conduct internal audits to ensure compliance with ISO/SAE 21434
- Implement lessons learned from incidents and near-misses

Documentation and Records

- Maintain comprehensive documentation of all cybersecurity activities
- Ensure proper version control and access management for sensitive documents

By implementing this policy, we aim to enhance the cybersecurity posture of our automotive products and comply with the requirements of ISO/SAE 21434. All employees are expected to adhere to this policy and report any cybersecurity concerns or incidents promptly.

6. Secure development and maintenance

Under analysis.