C1. Cybersecurity Threats

Description: The specific codes to represent a group of threats.

Code 1.1: General Requirements: Hardware security
Code 1.2: General Requirements: Software security
Code 1.3: General Requirements: Low-end OS (e.g., RTOS) on MCU
Code 1.4: General Requirements: High-end OS (e.g., Linux, Android) on MPU
Code 1.5: General Requirements: Data related
Code 1.6: In-vehicle Components: IVI
Code 1.7: In-vehicle Components: Telematics
Code 1.8: In-vehicle Components: Sensors
Code 1.9: In-vehicle Components: Gateway and Zone Controller
Code 1.10: In-vehicle Components: Advanced driver-assistance system (ADAS)
Code 1.11: In-vehicle Components: In-Vehicle Network (IVN)
Code 1.12: In-vehicle Components: Battery Management System (BMS)
Code 1.13: In-vehicle Components: Other ECUs
Code 1.14: Outside-vehicle components: Mobile App.
Code 1.15: Outside-vehicle components: Backend Server.
Code 1.16: Outside-vehicle components: Charging pile.
Code 1.17: Communication protocols: Short-range communication protocols: UWB, NFC, and BLE.
Code 1.18: Communication protocols: V2X.
Code 1.19: Communication protocols: In-vehile CAN.
Code 1.20: Communication protocols: In-vehicle Ethernet.
Code 1.21: Communication channel/interface: Wireless channels - Wi-Fi, Bluetooth, and Cellular.
Code 1.22: Communication channel/interface: Physical - Charging port.
Code 1.23: Communication channel/interface: Physical - USB and SD card.
Code 1.24: Communication channel/interface: Physical - OBD port.
Code 1.25: Vehicular function/services: OTA update.
Code 1.26: Vehicular function/services: Diagnostic.
Code 1.27: Vehicular function/services: Remote monitor and control.
Code 1.28: Other threats.

C2. Cybersecurity Responsibilities

Description: The specific responsibilities of the participant.

C2.1: Security baseline testing: Testing the security of a system by establishing a baseline configuration, then assessing any deviations from that baseline and identifying potential vulnerabilities.

C2.2: Penetration testing: A type of security testing where trained professionals attempt to exploit vulnerabilities in a system to identify potential risks.

C2.3: Threat Analysis and Risk Assessment (TARA): A process for identifying potential threats to a system and assessing the risks associated with those threats.

C2.4: Project Manager: An individual responsible for overseeing and coordinating the planning, implementation, and monitoring of a project to ensure it meets its goals and objectives.

C2.5: Regulation Study: A systematic analysis of the laws, guidelines, and standards related to a particular industry or domain, to determine their applicability, relevance, and impact on the relevant stakeholders.

C3. Groups & Stakeholders

Description: The various groups and stakeholders the participants met with in their work.

C3.1: Security testing group: A team responsible for conducting tests and assessments to identify and mitigate vulnerabilities in a vehicle's cyber-physical systems, ensuring the security of automotive software and hardware.

C3.2: Threat Analysis and Risk Assessment group: A group that analyzes potential cyber threats and assesses risks to automotive systems, helping to prioritize and implement necessary security measures.

C3.3: Development group: The team responsible for designing, building, and maintaining the software and hardware components of vehicles, ensuring that automotive cybersecurity best practices are integrated throughout the development process.

C3.4: Sales group: The division that markets and sells vehicles and automotive services, ensuring that customers are well-informed about the cybersecurity features and benefits of their products.

C3.5: Third-party Testing agency: An independent organization that conducts unbiased security assessments and evaluations of automotive systems to validate and improve their cybersecurity posture.

C3.6: Third-party consulting group: An external team of experts that provides automotive companies with cybersecurity guidance, strategy, and support, helping to ensure the security of vehicles and connected infrastructure.

C4. Security Activity Implementation

Description: concepts involved in discussing security activity implementations.

C4.1: Job Content and Regulations: Examination of how existing regulations relate to specific job content (e.g., TARA, testing, or management), including references to specific threat scenarios, TARA methods, and other provisions in ISO 21434.

C4.2: Regulation Implementation: Discussion on how the content of existing regulations is implemented to ensure product cybersecurity, such as referencing specific threat scenarios, interpreting and translating the TARA method, and implementing high-level requirements in ISO 21434 clauses.

C4.3: Security Baseline Compliance: Analysis of how teams ensure products meet the security baseline specified by current regulations in the context of increasingly complex automotive systems.

C4.4: Supply Chain Security: Exploration of how teams ensure supply chain security and the specific challenges faced by first-party OEMs and third-party suppliers in meeting security requirements.

C4.5: Cross-Team Collaboration: Discussion on how various teams collaborate to ensure automotive cybersecurity and the specific challenges faced in collaborating with internal and external teams.

C4.6: Cybersecurity Activity Challenges: Identification of specific challenges that hinder teams from carrying out cybersecurity activities, such as insufficient budgets or lack of prioritization by other teams.

C4.7: Latest Knowledge Integration: Examination of how teams effectively integrate the latest knowledge in the field of automotive cybersecurity, including obtaining information from security reports, research papers, or communicating with other teams and companies.

C4.8: Knowledge Acquisition Challenges: Discussion on the challenges encountered while acquiring the latest knowledge in automotive cybersecurity, such as difficulty in correlating knowledge with specific vehicular systems, inconsistent quality of materials, or limited access to information.

C4.9: Information Synchronization: Analysis of whether problems with information synchronization between security and non-security teams, such as understanding specific threats, are often encountered in the work process.

C4.10: Other Cybersecurity Challenges: Open-ended question regarding any other challenges faced by teams while conducting cybersecurity activities.

C5. Threat Analysis and Risk Assessment (TARA)

Description: concepts involved in discussing TARA.

C5.1: Asset identification: The process of recognizing and cataloging critical components, systems, and data within a vehicle that need to be protected from potential cybersecurity threats.

C5.2: Threat scenario identification: The act of defining and outlining possible cyber-attack scenarios that could target automotive systems, based on known vulnerabilities and threat actors.

C5.3: Impact rating: The evaluation of the potential consequences and severity of a successful cyber-attack on a vehicle's assets, taking into account factors such as safety, privacy, and financial loss.

C5.4: Attack path analysis: The examination of the various routes and methods a cyber-attacker might use to compromise automotive systems, helping to identify potential weaknesses and points of entry.

C5.5: Attack feasibility analysis: The assessment of the likelihood and practicality of a specific cyber-attack being executed against a vehicle's assets, considering factors like attacker skill level and available resources.

C5.6: Risk value determination: The process of estimating the overall risk associated with a particular threat scenario in automotive cybersecurity, based on the likelihood of an attack, its potential impact, and existing security controls.

C5.7: Risk treatment decision-making: The selection and prioritization of appropriate countermeasures, strategies, and security controls to manage and mitigate identified risks to automotive systems and assets.

C6. Evaluating Threat Descriptions

Description: concepts involved in discussing particular threats.

C6.1: Affected Asset (AA): The term "AA" denotes the particular automotive asset impacted by the threat, which could be an in-vehicle ECU (such as IVI or Telematics) or functions closely related to cybersecurity (like FOTA or remote control).

C6.2: Attack Description (AD): "AD" refers to the detailed description of the attack in the context of the threat, and it should encompass three elements: the Attack Vector (the channel through which the attacker can initiate the attack), Attack Method (the approach the attacker can use to execute the attack), and Attack Impact (the resulting consequences or damages from the attack).

C6.3: Root Cause (RC): The term "RC" refers to the underlying cause of the threat, specifically, the particular vulnerability and reason that led to the threat's existence.

C6.4: Security Testing Approach (STA): "STA" denotes the specific testing method that can be employed to detect the threat, examples of which include fuzzing and penetration testing.

C6.5: Mitigation (MG): The term "MG" describes the countermeasures that can be put in place to safeguard the system from the threat.

C7. Limitations and Recommendations

Description: concepts involved in open-ended discussion on regulations.

C7.1: Assessment Results: Evaluation of the quantity and quality of threats in existing automotive cybersecurity standards and regulations, and identification of any limitations in quantity or quality.

C7.2: Current Regulations: Analysis of whether current regulations provide practical and effective specific threats for automotive systems or if these threats are largely borrowed from other domains (e.g., mobile security, server security).

C7.3: Objective Assessment Criteria: Discussion on whether the absence of objective and unified assessment criteria leads to inconsistencies in security implementation.

C7.4: Threat Prioritization: Examination of whether there is a lack of prioritization for specific threats, making it difficult for manufacturers to determine the severity and priority of threats.

C7.5: Threat Descriptions: Evaluation of whether current threat descriptions are clear enough to help understand threats in specific contexts (e.g., attack paths shown in ISO 21434).

C7.6: Security Testing Guidance: Analysis of whether current regulations provide effective guidance for security testing.

C7.7: Mitigation Measures: Discussion on whether existing regulations' mitigation measures resemble remediation actions post-attack and if advanced security solutions should be adopted during early development stages.

C7.8: Black-Box and Gray-Box Scenarios: Examination of whether current threats and testing methods focus more on black-box and gray-box scenarios, and if more specific guidance for white-box scenarios would be beneficial (e.g., when manufacturers have access to the source code of ECUs).

C7.9: Threat Currency: Analysis of whether the threats provided in current regulations are up-to-date, or if they have not kept pace with the rapid development of the industry.

C7.10: Cybersecurity and Functional Safety Testing: Identification of any gaps between cybersecurity testing and functional safety testing, and comparison of the challenges in establishing effective safety testing standards versus security testing.

C7.11: Testing Method Practicality: Evaluation of whether the testing methods in current regulations can be practically applied to real products, or if they are too idealized and cannot meet the implementation needs of various vehicle models.

C7.12: Impact Scope Description: Assessment of whether the impact scope description of specific threats is sufficient, considering the interconnected nature of various ECUs in IVN topology, and how a threat on one ECU may lead to another threat on a specific ECU.