Threat Analysis and Risk Assessment (TARA)

Product: Transmission Control Unit (TCU)

Organization: ACH | **Tool:** QuickTARA

Generated: 2026-02-08 09:20

Document Version: v3

Product Type: ECU | **Safety Level:** QM

Description: Controls gear shifting in automatic and semi-automatic transmissions. Optimizes performance, fuel efficiency, and smoothness of shifting the vehicle.

This document satisfies ISO/SAE 21434:2021 TARA documentation requirements for regulatory submission.

ISO/SAE 21434:2021 Compliance Statement

This TARA report fulfills the following ISO/SAE 21434:2021 requirements:

Work Product	Clause	Requirement	Report Section
WP-09	9.4	Risk Assessment Report	Risk Assessment Summary
WP-10	10.4	Cybersecurity Goals	Cybersecurity Goals
WP-09	9.3	Risk Treatment Decisions	Risk Treatment Decisions
WP-09	9.2	Risk Determination	Risk Assessment Matrix
WP-08	8.4	Threat Scenarios	Threat Scenarios
WP-07	7.4	Damage Scenarios	Damage Scenarios
WP-06	6.4	Asset Identification	Traceability Matrix

Risk Assessment Summary (WP-09 9.4)

This section summarizes the assessed damages and risk treatment decisions.

Damage Severity (count)

Severity	Count
Critical	6
High	15
Medium	12
Low	1

Risk Levels (count)

Risk Level	Count
Critical	3
Medium	11
Low	3
High	4

Treatment Status (count)

Status	Count
draft	17
approved	4

Approved Treatments: 4

Assets Overview

Total assets: 9

ID	Name	Description
AS-008	Boot Loader	Secure boot loader for firmware updates and validation
AS-002	CAN Bus Interface	Communication interface for vehicle network protocols
AS-004	Calibration Data	Engine calibration parameters and lookup tables
AS-005	Configuration Settings	System configuration and operational parameters
AS-003	Diagnostic Software	On-board diagnostic system for fault detection
AS-001	Engine Control Firmware	Main ECU firmware controlling engine parameters and fuel injection
AS-007	Security Module	Hardware security module for cryptographic operations
AS-006	Sensor Data Interface	Interface for reading sensor values and environmental data
asset_630e9c04	Test Calib	Test

Damage Scenarios Analysis

Total damage scenarios identified: 34

ID	Name	Description	SFOP Rating
DS-001	Engine Control Firmware Corruption	Malicious modification of engine control firmware leading to unsafe engine operation	Severe

DS-002	CAN Bus Message Injection	Unauthorized injection of malicious CAN messages disrupting vehicle communication	Major
DS-003	Diagnostic Data Exposure	Unauthorized access to sensitive diagnostic information and fault codes	Major
DS-004	Calibration Parameter Tampering	Modification of engine calibration data causing performance degradation	Severe
DS-005	Configuration Setting Manipulation	Unauthorized changes to system configuration affecting vehicle behavior	Major
DS-006	Sensor Data Spoofing	False sensor readings causing incorrect system responses	Major
DS-007	Security Module Compromise	Breach of hardware security module exposing cryptographic keys	Severe
DS-008	Boot Loader Bypass	Circumvention of secure boot process allowing unauthorized firmware	Severe
DS-009	Firmware Rollback Attack	Downgrade to vulnerable firmware version with known exploits	Major
DS-010	CAN Bus Denial of Service	Flooding CAN network with messages causing communication failure	Severe
DS-011	Diagnostic Port Exploitation	Unauthorized access through diagnostic interface for system manipulation	Major
DS-012	Calibration Data Corruption	Accidental or malicious corruption of critical calibration parameters	Major
DS-013	Configuration Backup Exposure	Unauthorized access to configuration backup files revealing system details	Moderate
DS-014	Sensor Interface Jamming	Electronic interference disrupting sensor data collection	Major
DS-015	Cryptographic Key Extraction	Physical or side-channel attacks extracting encryption keys	Severe
DS-016	Firmware Update Interception	Man-in-the-middle attack during firmware update process	Major
DS-017	CAN Message Replay Attack	Recording and replaying legitimate CAN messages at inappropriate times	Major
DS-018	Diagnostic Log Tampering	Modification of diagnostic logs to hide malicious activities	Major
DS-019	Calibration Version Mismatch	Installation of incompatible calibration data causing system instability	Major
DS-020	Configuration Factory Reset Abuse	Unauthorized factory reset exposing default credentials	Major
DS-021	Firmware Memory Overflow	Buffer overflow in firmware causing system crash or code execution.	Major
DS-022	CAN Bus Timing Attack	Exploitation of CAN message timing to infer sensitive informationd	Major
DS-023	Diagnostic Interface Brute Force	Brute force attack on diagnostic authentication mechanismsd d	Major

DS-024	Calibration Checksum Bypass	Bypassing integrity checks on calibration data	Major
DS-025	Configuration Privilege Escalation	Exploiting configuration system to gain elevated privileges	Major
DS-026	Sensor Calibration Drift	Gradual sensor calibration drift causing inaccurate readings	Major
DS-027	Hardware Security Module Fault Injection	Physical fault injection attacks on security hardware	Severe
DS-028	Boot Chain Verification Bypass	Circumventing boot chain integrity verification	Severe
DS-029	Firmware Debug Interface Exposure	Unauthorized access through exposed debug interfaces	Major
DS-030	CAN Network Segmentation Failure	Failure of network segmentation allowing cross-domain access	Severe
DS-031	Diagnostic Command Injection	Injection of malicious commands through diagnostic interface	Major
DS-032	Calibration Data Race Condition	Race condition in calibration data access causing corruption	Major
DS-033	Configuration Backup Poisoning	Malicious modification of configuration backup files	Major
DS-034	Sensor Fusion Algorithm Manipulation	Tampering with sensor fusion algorithms affecting decision making	Major

SFOP rating: Severe = highest damage impact; Major = significant impact; Moderate = limited impact; Negligible = minimal impact.

Cybersecurity Goals (WP-10)

ISO 21434 requires cybersecurity goals for Medium, High and Critical risks that have been approved for acceptance:

Goal ID	Risk Treatment Decision	Cybersecurity Goal
CG001	Retaining	Many times risks are risks
CG002	Reducing	Ensure diagnostic data confidentiality by implementing encrypted communication protocols and access controls for the OBD-II diagnostic interface.
CG003	Retaining	The Goal is goaling
CG004	Reducing	Ensure we are good