Cybersecurity Case iso175
(in accordance with ISO/SAE 21434 and UNECE R155)

1. Purpose and Scope

This document presents the Cybersecurity Case for the product iso175. It serves as a structured demonstration that cybersecurity requirements from UNECE R155 and ISO/SAE 21434 have been appropriately addressed during development, integration, and intended operation. It does not replace a type approval but contributes to the overall cybersecurity evaluation performed by the vehicle manufacturer.

Scope:

- Product: iso175 (see Annex)
- Variants: see Annex
- Target Markets: Global (including UNECE and non-UNECE countries)

2. Reference Standards and Regulations

- UNECE R155 (Cybersecurity Management System - “CSMS”)
- ISO/SAE 21434:2021 – Chapters 6, 9, 10, 11

3. Product-specific Cybersecurity Strategy

The iso175 is a permanently integrated, static, non-updatable component. It communicates only within the internal CAN system and has no wireless, cloud, or OTA interfaces. Cybersecurity risks result exclusively from its integration into the vehicle's electrical architecture.

4. Summary of Threat Analysis and Risk Assessment (TARA)

The detailed risk assessment of the threats listed below is documented in the *Cybersecurity Safety Manual iso175, Version 2.0, dated 04.07.2025*. That document includes all threat scenarios with their evaluation (Impact, Feasibility, Risk Level) and recommended mitigations. The following summary presents the identified threats in qualitative form:

Amtsgericht Gießen HRA 1159
Pers. haftende Gesellschafterin:
Dipl.-Ing. Wilshaus GmbH
Amtsgericht Gießen HRB 173
Sitz der Gesellschaft: Grünberg
USt-IdNr. DE112643173

Geschäftsführer: Michael Breuer,
Nicole Bender, D. Christian Bender

Prokurist: Christian Jerkel

WEEE-Reg.-Nr. DE 43 124 402

Commerzbank Gießen
IBAN: DE32 5134 0013 0205 2520 00
BIC: COBADEFFXXX
Sparkasse Grünberg
IBAN: DE88 5135 1526 0000 0119 08
BIC: HELADEF1GRU

Deutsche Bank Gießen
IBAN: DE36 5137 0008 0023 7008 00
BIC: DEUTDEFF513
Volksbank Mittelhessen
IBAN: DE59 5139 0000 0046 6823 00
BIC: VBMHDE5FXXX

#	Threat	Recommended mitigation (see Safety Manual)
1	Manipulation of safety-relevant parameters via CAN	Physical CAN isolation, reduced number of nodes, short bus length
2	Firmware manipulation	Evaluate all alarm flags to detect modified firmware states
3	Busy CAN / Denial of Service	Host-side watchdog to detect missing cyclic CAN messages

5. Cybersecurity Goals and Claims

The iso175 addresses the following cybersecurity goals:

- Prevent manipulation via CAN (by physical isolation)
- Detect firmware tampering (via internal alarm flags)
- Ensure CAN availability (via host-side watchdog)

System-level implementation and monitoring lie with the OEM.

6. Supporting Documentation and Evidence

The following documents are provided by Bender GmbH & Co. KG and are available for download on the company website:

- Cybersecurity Safety Manual
- CAN Communication Specification

7. Residual Risk Evaluation

From the manufacturer's perspective, no unacceptable risks exist for the intended use. Integration into a UNECE R155-compliant vehicle system by the OEM is therefore considered feasible.

8. Responsibility and System Integration

The OEM is responsible for system-level integration, protection of interfaces, and compliance with the overall CSMS.

9. Applicability to UNECE R156

The iso175 has no software update capability. Neither OTA nor workshop-based updates are supported or technically possible. The device is a static system with no update mechanism. Therefore, UNECE R156 does not apply to this component.

10. Disclaimer

This document is not a formal type approval certificate. It is intended solely to support cybersecurity evaluation during vehicle integration. Improper use or system integration beyond the intended design is not within the responsibility of the manufacturer.

11. Approval

Grünberg, July 10, 2025

Signed by:
Ulrich von Waldow
C3831F0095374D5...
(U. Waldow, Lead Developer Cybersecurity)

Signiert von:
Björn Burger
8F9B44CDB577467...
(B. Burger, Product Manager)

12. Annex

Annex – Type Overview		
Product Group	**Part. No.**	**Product Designation**
iso175C	B91068201	iso175C-32-SS
iso175C	B91068202	iso175C-42-SS
iso175C	B91068203	iso175C-32-SB
iso175C	B91068204	iso175C-42-SB
iso175C	B91068200	iso175C – customer specific version