Cybersecurity Safety Manual

(Version 2.0, 04.07.2025)

Content

1 General 2
2 Remaining risks 2
2.1 Manipulation of safety relevant parameters 2
2.1.1 Attack scenario 2
2.1.2 Risk 2
2.1.3 Recommended actions 2
2.2 Manipulation of firmware 3
2.3 Attack scenario 3
2.3.1 Risk 3
2.3.2 Recommended actions 3
2.4 Busy CAN bus communication 3
2.4.1 Attack scenario 3
2.4.2 Risk 4
2.4.3 Recommended action 4

1 General

The purpose of this document is to list all remaining risks after the TARA analysis and gives advice for increasing the detection of modifications related to firmware or safety relevant parameters. Also, where possible, advice for lowering the feasibility is given.

Lowering the impact of an attack is not possible, because an electrical shock could always lead to death independent of the already implemented measures. Only the possibility that such an event could take place can be lowered.

2 Remaining risks

2.1 Manipulation of safety relevant parameters

2.1.1 Attack scenario

In case an attacker has access to the CAN bus he can modify safety relevant parameters by sending related CAN bus messages.

2.1.2 Risk

The risk for that treatment scenario was rated as 3 (impact: Severe, Feasibility: low).

2.1.3 Recommended actions

The physical CAN bus should not be easily accessible from outside the vehicle. The number of bus clients should be as low as possible. In the best case only the BMS (Battery management system) is connected to the iso175 using an electrical separated CAN bus.

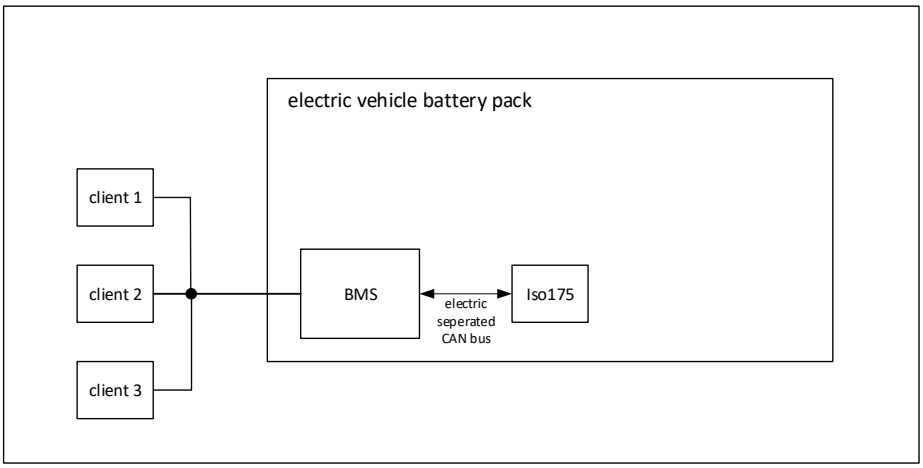

Figure 1: Block diagram Iso175 Interface connection

2.2 Manipulation of firmware

2.3 Attack scenario

In case an attacker has access to the original firmware, he can modify relevant parts of it.

2.3.1 Risk

The risk for that treatment scenario was rated as 3 (impact: Severe, Feasibility: low)

2.3.2 Recommended actions

Because of already implemented functions for detecting modified firmware the user shall evaluate all alarm flags and not only alarm flags related to an insulation error.

2.4 Busy CAN bus communication

2.4.1 Attack scenario

In case an attacker has access to the electric CAN bus he can generate high CAN bus traffic so that no message from the iso175 is transferred (lower priority).

2.4.2 Risk

The risk for that treatment scenario was rated as 3 (impact: Severe, Feasibility: low)

2.4.3 Recommended action

The host controller should observe that CAN messages from the Iso175 are cyclic transmitted. In case for a specified time no new CAN massage was received from the Iso175 the host should react in that case.