TRIAL COPY — NOT FOR OFFICIAL USE

Cybersecurity Concept

AEB System — Public Synthetic Demonstration

Aligned with ISO/SAE 21434; UN R155
Domain: automotive · Scope: system-function
Scoring method: Attack Potential (ISO/IEC 18045)
Generated 2026-10-28T08:00:00.000Z · TARAexl 0.1.64

Trial copy — not for official use

1. Document Information

Project	AEB System — Public Synthetic Demonstration
Document ID	TARA-AEB-DEMO-001
Version	1.0
Status	draft
Classification	Public synthetic demonstration — not a production assessment
Standard	ISO/SAE 21434; UN R155
Generated	2026-10-28T08:00:00.000Z

DRAFT — this document contains only approved analysis content but has not been released. It is a working state for review purposes and shall not be used as evidence of a completed risk assessment. Distribution is limited by the classification "Public synthetic demonstration — not a production assessment".

Role	Name	Date
Author	Demonstration author	
Reviewer	Demonstration reviewer	
Cybersecurity manager	Demonstration cybersecurity manager	

2. Item Overview

ITM-1 — Automatic Emergency Braking (AEB) System
The AEB ECU fuses front-radar and front-camera data to detect an imminent collision and commands the brake system to decelerate the vehicle when the driver does not react in time.
Functions: Detect an imminent forward collision by fusing front-radar and front-camera perception; Command an autonomous emergency brake application when a collision is otherwise unavoidable; Warn the driver before the system intervenes

3. Scope & Assumptions

ID	Description	Impact if incorrect	Status
ASM-1	The radar and camera are independent sensors, so a single spoofing technique cannot fool both at once.	The sensor-fusion plausibility argument and its residual risk would change.	open
ASM-2	The UDS security-access seed-key algorithm is confidential and unique per vehicle line.	The feasibility of calibration tampering rises from medium towards high.	open

4. Summary of Main Cybersecurity Risks

Risk	Damage	Risk level	Value	CAL	Impact	Feasibility
R-1	DS-1	high	4	2	Severe	medium
R-2	DS-2	high	4	4	Major	high
R-3	DS-3	high	3	2	Major	medium
R-4	DS-4	medium	3	3	Moderate	high

5. Risk Treatment

Risk	Treatment	Proposed controls	Residual feasibility	Residual risk	Sign-off
R-1	reduce	Cross-check radar against camera and reject implausible	low	Reduced to medium after fusion plausibility checks.	Required

Trial copy — not for official use

Risk	Treatment	Proposed controls	Residual feasibility	Residual risk	Sign-off
		single-sensor perception before braking.; 2 linked control(s)			
R-2	reduce	Authenticate the chassis-CAN brake request with SecOC (freshness + MAC).; 1 linked control(s)	low	Reduced to low.	Not required
R-3	reduce	Strengthen UDS security access, accept only signed calibration datasets, and reject out-of-range safety thresholds.; 2 linked control(s)	low	Reduced to low: unsigned or implausible calibration is refused.	Not required
R-4	reduce	Reserve top bus priority for the warning frame, rate-limit at the body gateway, and latch the warning in the cluster on first reception.; 2 linked control(s)	low	Reduced to low: a flood no longer displaces the warning in time.	Not required

6. Cybersecurity Goals

ID	Related risks	Goal
GL-1	R-1	The AEB shall brake only on perception that is integrity-protected and plausibility-checked.
GL-2	R-1, R-2	Emergency-brake requests shall be authenticated on the chassis CAN.
GL-3	R-3	Safety-relevant AEB calibration shall be modifiable only through authenticated, integrity-protected diagnostic sessions.
GL-4	R-4	The forward-collision warning shall remain available under bus-flooding conditions.

Trial copy — not for official use

7. Cybersecurity Requirements

ID	Requirement	Type	Responsible element	Verification
RQ-1	The AEB ECU shall fuse radar and camera and reject implausible single-sensor detections before braking.	technical	AEB ECU	test
RQ-3	Calibration writes shall require UDS security access and a signed calibration dataset; out-of-range safety thresholds shall be rejected and logged.	technical	AEB ECU	test
RQ-4	The forward-collision warning shall use a reserved top-priority identifier, and the instrument cluster shall latch a received warning within 100 ms.	technical	Instrument Cluster	test

8. Cybersecurity Claims

None approved/recorded.

9. Traceability Summary

Asset	Damage	Risk	Risk level	Treatment	Goals	Requirements	Claims
AST-1 — Forward perception object list	DS-1 — The AEB fails to brake for a real obstacle, leading to a collision and occupant injury.	R-1	high	reduce	GL-1 — The AEB shall brake only on perception that is integrity-protected and plausibility-checked. | GL-2 — Emergency-brake requests shall be authenticated on the chassis CAN.	RQ-1 — The AEB ECU shall fuse radar and camera and reject implausible single-sensor detections before braking.	—
AST-2 — Emergency	DS-2 — Unintende	R-2	high	reduce	GL-2 — Emergency	—	—

Trial copy — not for official use

Asset	Damage	Risk	Risk level	Treatment	Goals	Requirements	Claims
brake command	d emergency braking triggers a rear-end collision.				-brake requests shall be authenticated on the chassis CAN.		
AST-3 — AEB calibration parameters	DS-3 — Tampered calibration makes the AEB brake late or spuriously, degrading collision protection until the next service.	R-3	high	reduce	GL-3 — Safety-relevant AEB calibration shall be modifiable only through authenticated, integrity-protected diagnostic sessions.	RQ-3 — Calibration writes shall require UDS security access and a signed calibration dataset; out-of-range safety thresholds shall be rejected and logged.	—
AST-4 — Forward-collision warning	DS-4 — The driver receives no forward-collision warning, so the autonomous intervention arrives unannounced.	R-4	medium	reduce	GL-4 — The forward-collision warning shall remain available under bus-flooding conditions.	RQ-4 — The forward-collision warning shall use a reserved top-priority identifier, and the instrument cluster shall latch a received warning within 100 ms.	—

10. Residual Risk Summary

Risk	Original risk	Treatment	Main controls	Residual feasibility	Residual risk	Sign-off
R-1	high	reduce	Cross-check radar against camera and reject implausible single-sensor perception before	low	Reduced to medium after fusion plausibility checks.	Required

Trial copy — not for official use

Risk	Original risk	Treatment	Main controls	Residual feasibility	Residual risk	Sign-off
			braking.; 2 linked control(s)			
R-2	high	reduce	Authenticate the chassis-CAN brake request with SecOC (freshness + MAC).; 1 linked control(s)	low	Reduced to low.	Not required
R-3	high	reduce	Strengthen UDS security access, accept only signed calibration datasets, and reject out-of-range safety thresholds.; 2 linked control(s)	low	Reduced to low: unsigned or implausible calibration is refused.	Not required
R-4	medium	reduce	Reserve top bus priority for the warning frame, rate-limit at the body gateway, and latch the warning in the cluster on first reception.; 2 linked control(s)	low	Reduced to low: a flood no longer displaces the warning in time.	Not required

11. Open Points & Missing Information

Source	Related to	Description	Owner	Priority	Status
Assumption	R-1	The radar and camera are independent sensors, so a single spoofing technique cannot fool both at once.			open
Assumption	R-3	The UDS security-access seed-key algorithm is confidential			open

Trial copy — not for official use

Source	Related to	Description	Owner	Priority	Status
		and unique per vehicle line.			

12. Software Bill of Materials

Name	Version	Supplier	License
zlib	1.2.11	zlib project	Zlib
openssl	3.0.12	OpenSSL Project	Apache-2.0
mbedtls	3.5.0	TrustedFirmware	Apache-2.0
FreeRTOS	10.6.1	Amazon Web Services	MIT
lwip	2.2.0	lwIP project	BSD-3-Clause
tinycbor	0.6.0	Intel	MIT

None approved/recorded.

Trial copy — not for official use