This is for example purposes only. BH's TARA reports provides more detailed analysis than what is displayed here

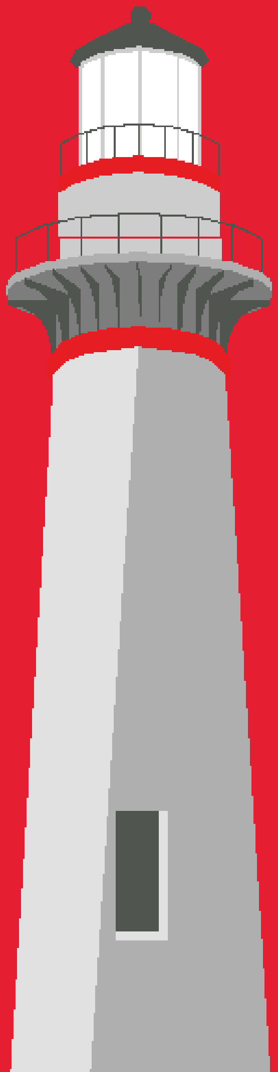
X.XX.XXX

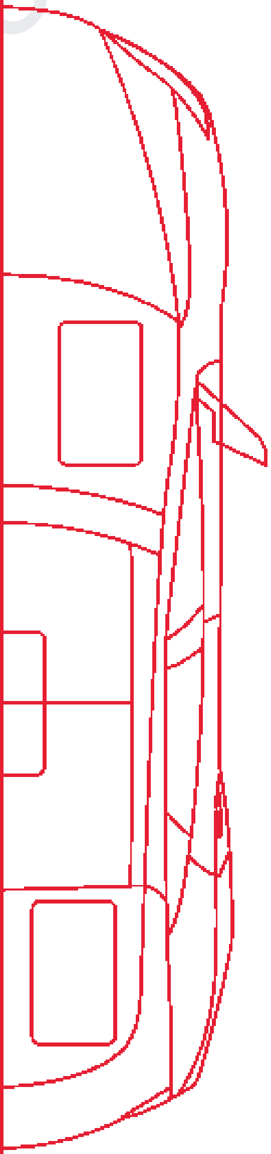
Draft Report

SECURITY ASSESSMENT

Threat Analysis Risk Assessment (TARA)

Driver Attention Monitoring Feature





Block Harbor.
Cybersecurity

Table of Contents

Project Info: Driver Attention Monitoring Feature [DAM]

Project Data

Target Of Evaluation	Contributing system Driver Attention Monitoring feature
Project	XXXXXX Program
Contact (Department)	Block Harbor Cybersecurity
Contact (Security Expert)	XXXXXX
Editor	XXXXXX
Deadline	-

Status

Risk Analysis Status	In Review

Version History

Revision	Date	Authors	Description
1	XXXXXX	XXXXXX	Review ready version.

Executive Summary

Purpose and Scope

The purpose of the Threat Analysis and Risk Assessment (TARA) is to identify new and evolving cybersecurity risks for vehicles early in the engineering process and updated throughout the life of the vehicle for regulatory compliance and standard conformance. Block Harbor Cybersecurity utilizes a standard methodology to perform item definition and a corresponding security analysis to ensure completeness of the TARA. The outcomes of the TARA are the finite cyber-physical assets with known risk values associated with the product to make them manageable during the entire product lifecycle at scale. The risk table lists potential incidents or product failures that will affect overall product quality. Each risk identified in this TARA report should be accepted, reduced, mitigated, or transferred. This report conforms with ISO/SAE 21434:2021 as a formal work product that may be used as evidence for UNECE WP.29 R155 type approval.

Block Harbor is an independent third-party company, conducting a System Level TARA (Threat Analysis and Risk Assessment), by thoroughly examining the documentation and reports that comprise the item definition in this report. Specified scope of the:

- **Driver Attention Monitoring (DAM) System**

Methodology

This document is intended to fulfill the requirements for a Threat Analysis and Risk Assessment (TARA) with recommended rigor to produce outcomes described by ISO/SAE 21434:2021. This inductive analysis does not consider, supersede, or take into account any other TARA's which may contribute other feature threats or controls. This report first covers the item definition. The item definition provides details regarding the context in which the asset exists, operates, and can be compromised due to misuse of the product. To achieve this, we include in the report the:

- Target of Evaluation system level overview
- Functions list
- Assets in relation to functions and relevant elements
- Declaration of elements: Components, Channels, Data, Data Flows

After getting an understanding of the assets within the item boundary, the content is presented in two parts in the order which the analysis is conducted:

1. Threat Analysis:
   - Damage scenarios with Impact ratings based on Safety, Financial, Operational, and Privacy (SFOP) damages
   - Threat Scenarios identified using Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation Privilege (STRIDE) with Feasibility ratings based on Elapsed Time, Special Expertise, Knowledge of Item, Window of Opportunity, and Equipment.
2. Risk determination:
   - Damage scenarios are declared as discrete risks with a cumulative risk rating according to the worst-case potential Impact and Feasibility. This risk determination is made assuming no mitigation measures in the form of E/E architectural design controls are implemented to mitigate those potential damages.
   - Risk determination is provided based on concept functions and preliminary design documentation.
   - Risks may be adjusted based on existing controls and assumptions.

Reference Documentation

- **Regulatory/Standards:**
  [1] ISO/SAE 21434:2021
  [2] UNECE WP.29 R155 type approval
- **Customer Internal Documents:**

1. **Document 1**
2. **Document 2**

Relevant Work Products from ISO/SAE 21434

- [WP-09-01] Item definition, resulting from the requirements of 9.3.2
- [WP-09-02] TARA, resulting from [RQ-09-03] and [RQ-09-04]
- [WP-15-01] Damage scenarios, resulting from [RQ-15-01]
- [WP-15-02] Assets with cybersecurity properties, resulting from [RQ-15-02]
- [WP-15-03] Threat scenarios, resulting from [RQ-15-03]
- [WP-15-04] Impact ratings with associated impact categories, resulting from [RQ-15-04] to [RQ-15-06]
- [WP-15-05] Attack paths, resulting from [RQ-15-08] and [RQ-15-09]
- [WP-15-06] Attack feasibility ratings, resulting from [RQ-15-10]
- [WP-15-07] Risk values, resulting from [RQ-15-15] and [RQ-15-16]
- [WP-15-08] Risk treatment decisions, resulting from [RQ-15-17]

Risk Distribution Table

The risk distribution below sums up the number of risks according to its corresponding impact level and feasibility level.
For example: There are 3 risks with a low feasibility and severe impact level

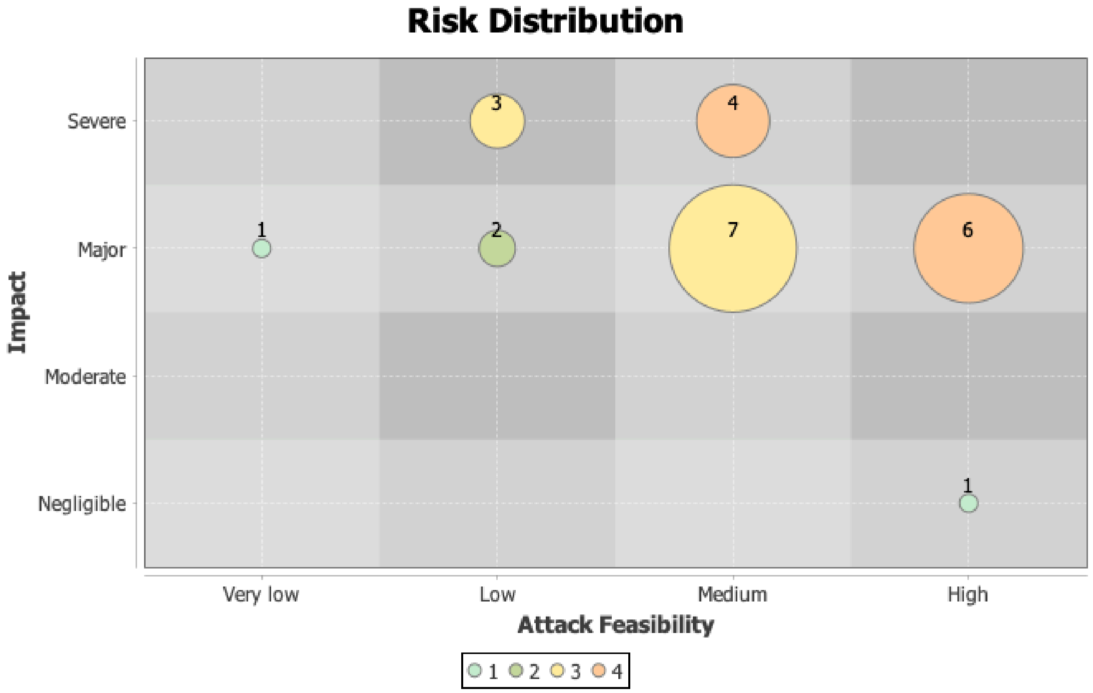


Figure 1 - Risk Distribution Matrix

Risk Table Before Controls

The following risks are summarized in the table below. The details of how each risk was identified can be traced in the remainder of the report.

Risk			Risk Level
Name	Title	Caused by	RL
R.1	Denial of Service	TS.1	3

Risk Levels After Controls

For purposes of convenience the below table is a selection of controls that are applied to each threat scenario to show reduced risk levels. However, for the comprehensive list of controls and control allocation, it is recommended that the technical work product of the cybersecurity concept [WP-09-06] be referenced.

Name	No Controls	Secure Boot	Secure UDS Diagnostics	ECU Hardening
R.1	3		1	

(End of Executive Summary)

(Start of Item Definition)

Diagram of DAM: Driver Attention Monitoring Onboard Vehicle Systems

The following is a visual representation of the feature with the vehicle as the root component represented on the outermost boundary as the root component. The target of evaluation is shown within the context of external nodes that contribute to the larger feature functionality. This Item Definition information is used to define the feature as the Target of Evaluation (ToE): in this case, the DAM is the target of evaluation.

The following tables include the list of elements with channels, components, data, data flows included in the item definition.

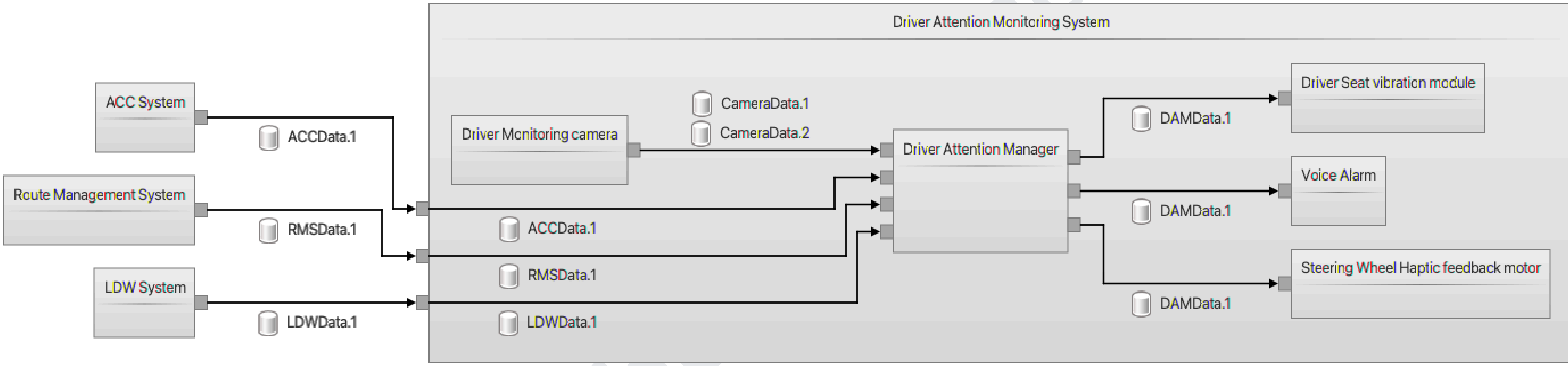


Figure 2 - Diagram of DAM

This is a SAMPLE document. All system elements are examples modeled from real world applications.

Functions Table

Name	Title	Description
F.1	Monitor User Attention	Monitor User Attention: Continuously monitors user attention levels to ensure they remain focused and not distracted during operation.
F.2	Engage Highly Automated Driving Mode	Allows the driver to engage HIGHLY AUTOMATED DRIVING MODE if proper conditions are met. Drivers can only activate the system after road conditions, current route, DAM sensor input, and calculated vehicle path have been validated by Driver Assist Subsystem.

Data Table

Name	Title	Description
ACCData.1	Acc Status	DAM receives a boolean value from ACC system based on information gathered from ACC system sensors which check vehicle speed, upcoming hazards, and driving distance relative to other objects perceived on the road, issuing a negative signal if the vehicle is relatively rapidly approaching an large object or hazardous environment.
CameraData.1	Eye Position Detection	Primary data value crucial to positively identifying if the driver is paying attention to the road.

Channels Table

Name	Title	Technology
DAM ACC	SYS4, Cmp.4 [CAN]	CAN: Controller Area Network
DAM DMC	Cmp.1, Cmp.4 [Eth]	Eth: Automotive Ethernet

Data Flows Table

Name	Title	Transferred Data
DF.1	DAMData.1: Cmp.4 -> Cmp.1 [LV hardwire]	DAMData.1: Alertdriver
DF.2	DAMData.1: Cmp.4 -> Cmp.1 [LV hardwire]	DAMData.1: Alertdriver

Assets and Damage Scenarios

The following is the allocation of feature assets that are vulnerable to potential damages due to malicious actions or unintentional misuse with the feature boundary. To effectively describe the damage potential, each asset is assigned with relevant security properties and assumptions on how the potential damage may be realized are listed as well based on the intended functionality on the vehicle level.

Components

Component (Asset)		Security Properties			Damage Scenarios	
Name	Title	C	I	A	Name	Title
Cmp.1	Driver Attention Monitoring System	-	X	-	DS.1	Driver Attention Monitoring system error causes vehicle collision
Cmp.4	LDW System	-	X	-	DS.1	Driver Attention Monitoring system error causes vehicle collision

Data Flows

Data Flow (Asset)		Security Properties		
Name	Title	C	I	A
DF.1	DAMData.1: Cmp.4 -> Cmp.1 [LV hardwire]	-	X	-
DF.2	DAMData.1: Cmp.1-> Cmp4 [LV hardwire]	-	X	-

.

(End of Item Definition)

(*Start of Threat Analysis)*

Assumptions Table

Assumptions are based on the architecture, intended use, and any other relevant information that are taken into consideration during the analysis.

Name	Title
AN.1	No OTA (Over The Air) Updates
AN.2	No Remote Access

Damage Scenarios Overview

The damage scenarios are assessed against potential adverse consequences in the impact categories of safety, financial, operational, and privacy (S, F, O, P) respectively. The classification is as follows:

Impact is the estimated damage or physical harm from a damage scenario. The impact level (**IL**) of a damage scenario is determined for each impact category as either severe, major, moderate, or negligible. The risk matrix below shows how the risk is calculated considering the impact rating and feasibility.

Damage Scenarios				
Name	Title	Description	Concerns	IL
DS.1	Driver Attention Monitoring system error causes vehicle collision	Tampering with the DAM cameras and sensors is not detected and Driver assistance (DAS) features are initialized under unsafe driving conditions.	I: DAM Cameras	Severe

Impact Breakdown per Damage Scenario

Damage Scenarios	Impact			
Name				
	S	F	O	P
DS.1	Severe	Moderate	Major	Negligible

Damage and Threat Scenarios Table

Damage Scenario		Threat Scenarios	
Name	Title	Name	Title
DS.1	Driver Attention Monitoring system error causes vehicle collision	AS.1	Tampering - Driver Monitoring camera
		AS.2	Information Disclosure - SYS1, Cmp.3, Cmp.4 [Eth]

Threat Scenarios and Descriptions

List of all the threat scenarios and threat descriptions.

Name	Title	Description
TS.1	Tampering with the Driver Monitoring Camera	Attackers can tamper with the DMC

Threat Scenarios and Attack Steps and Feasibility

Using an attack potential-based approach, the attack feasibility (**AF**) level is determined based on the mapping between attack potential and attack feasibility rating. The attack potential is the measure of the effort to be expended in attacking an item or component, expressed in terms of an attacker's expertise and resources. The attack feasibility rating is determined based on five core factors including specialist expertise, window of opportunity, elapsed time, equipment, and knowledge of the item. The rating is as follows:

Name	Title	Path	Steps	AFL
AS.1	Tampering - Driver Monitoring camera	AP.1	AS.1 Tampering - Driver Monitoring camera	Low
AS.2	Information Disclosure - SYS1, Cmp.3, Cmp.4 [Eth]	AP.1	AS.1: Tampering - Driver Monitoring camera	Low

Attack Steps Table

Name	Title	T	Ex	K	W	Eq	AFL
AS.1	Tampering - Driver Monitoring camera	T1	Ex1	K0	W0	Eq1	High

(End of Threat Analysis)

(*Start of Risk Analysis)*

Risks Table

For each threat scenario the risk level is determined from the impact of the associated damage scenarios and the attack feasibility of the associated attack paths. **Risk = Impact x Feasibility**

Risk				
Name	Title	Description	Caused by	RL
R.1	Spoofing - Eye Position, Head Position detection	Malicious actor injects positive Driver Attention Monitoring message to the DAM Manager module causing it to bypass the intended safe vehicle behavior.	AS.5: Spoofing - Eye Position detection, Head Position detection	3

(End of Risk Analysis)

(*Start of Risk Treatment)*

Controls Table

The following are three controls that have been applied to the applicable threat scenarios. However, for the comprehensive list of controls and control allocation, it is recommended that the technical work product of the cybersecurity concept [WP-09-06] be referenced.

Name	Title	Description	T	Ex	K	W	Eq	AFL
C.1	Secure Boot	The component shall generate a boot time integrity checking element (CMAC) .	T4	Ex2	K2	W2	Eq2	Very low
C.2	Secure UDS Diagnostics	This feature prevents UDS diagnostics features from being used by unauthorized entities.	T3	Ex2	K2	W2	Eq2	Very low

Risk Treatment Table

For each threat scenario, considering its risk values, one or more of the following risk treatment option(s) shall be determined:

a) avoiding the risk;

EXAMPLE: Avoiding the risk by removing the risk sources, deciding not to start or continue with the activity that gives rise to the risk.

b) reducing the risk;

c) sharing the risk;

EXAMPLE: Sharing risk through contracts or transferring risk by buying insurance.

d) retaining the risk.

NOTE: The rationales for retaining the risk and sharing the risk are recorded as cybersecurity claims and are subject to cybersecurity monitoring and vulnerability management in accordance with Clause 8.

Refer to the cybersecurity concept [WP-09-06] deliverable for the cybersecurity goal [WP-09-03] references and rationale for each residual risk.

Risk	Risk Level	Risk Treatment	Rationale
Driver attention loss causes rear collision of PassCar with Semi-trailer	Moderate (3)	No Controls implemented	Not available.

Block Harbor.

Cybersecurity