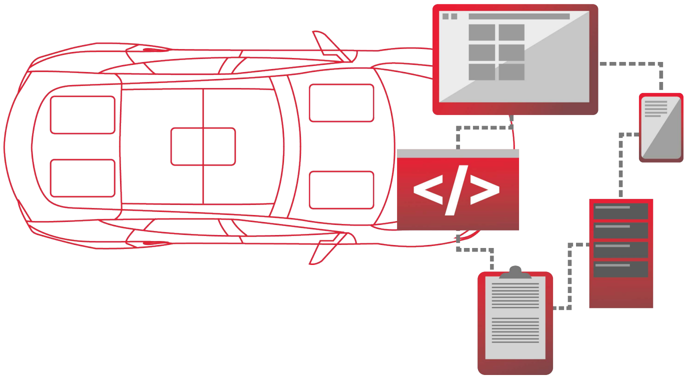
Vehicle, System, and Component Level Threat Analysis & Risk Assessment

TARA-as-a-Service to design vehicle cybersecurity with our expertise, tools, and efficiency.

The automotive industry is undergoing cybersecurity standardization and regulation that enforces consistent analysis to provide work products to auditors. Vehicles and their components that are cyber relevant must have a threat analysis and risk assessment (TARA) performed as a part of the cybersecurity design process.



What is TARA?

A TARA is an automotive-specific risk assessment process that fits within the ISO/SAE 21434 vehicle cybersecurity standard. Like any risk assessment, it starts with item definition to understand the assets being protected and where the boundaries exist. Then, damage scenarios for the item definition are identified based on safety, financial, operational, and privacy considerations. Then, threat scenarios are defined that may realize those damage scenarios and a likelihood is documented. Finally, a set of risks are documented based on the security analysis that is the outcome of the TARA. Those risks should guide the cybersecurity design.

Why Perform a TARA?

Security by Design

Instead of checking cybersecurity after the product has been developed, security by design is magnitudes more efficient and effective at ensuring the end product is secure. Plus, due to ISO/SAE 21434, your customers will ask for a TARA for your product. You need to be able to effectively secure the vehicle and adjust the TARA based on a changing threat and vulnerability landscape.

Challenges with TARA

Tools

Many companies are forced to create their own TARA template using tools like Excel because existing risk assessment tools do not fit automotive. At Block Harbor, we used industry-leading tools that specifically focus on ISO/SAE 21434 that let us focus on doing our job well.

Expertise

A cybersecurity design is only as good as the experts that are performing the TARA. Because TARA is done so early in the design process, it's critical that it's done right the first time.

Reusability

Many items and components have very similar TARAs. If you're managing multiple projects, being able to reuse different parts of TARAs speeds the process significantly.

Consistency

Each TARA may be different based on the knowledge and expertise of the security analyst performing the TARA. Being able to consistently perform, edit, and manage TARAs with a team of different analysts is critical to consistent cybersecurity.

Why Block Harbor?

Block Harbor was founded in 2014 in Detroit providing services to automakers and automotive suppliers to keep vehicles safe, ranging from penetration testing to running a 24/7/365 Security Operation Center (SOC). We're on a mission to build great solutions to keep mobility safe.

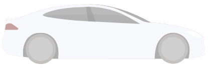
- Vehicle Cybersecurity Labs
  - -Penetration Testing
  - -Fuzzing
  - -V&V-as-a-Service
  - -Vehicle Cybersecurity Lab Buildout
- Vehicle Security Operations
  - -Vehicle Security Operation Center (VSOC)
  - -Threat Analysis and Risk Assessment (TARA)
  - -Vehicle Cybersecurity Management System (CSMS)
- Vehicle Cybersecurity Consulting

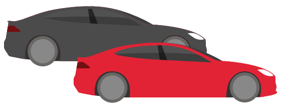
Block Harbor.
Cybersecurity

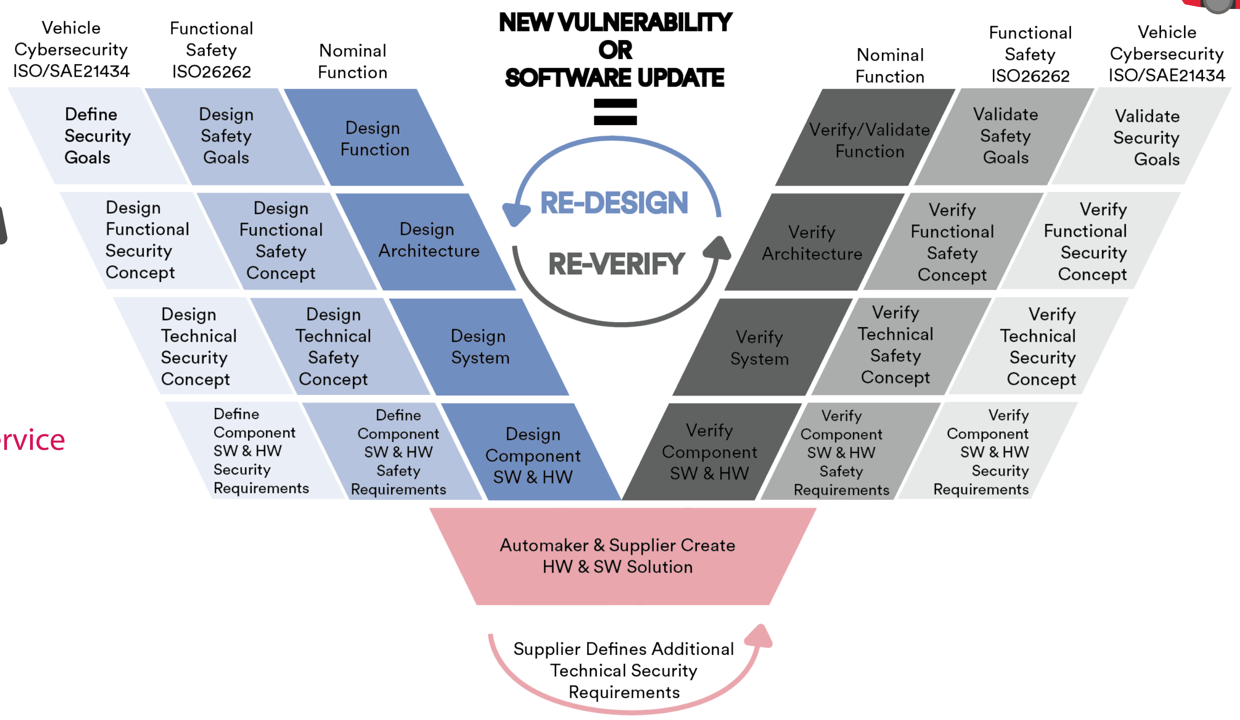
To learn more about working with our team to meet your vehicle security needs, please visit blockharbor.io

Vehicle, System, and Component Level Threat Analysis & Risk Assessment

TARA-as-a-Service to design vehicle cybersecurity with our expertise, tools, and efficiency.







Vehicle Cybersecurity ISO/SAE21434

Functional Safety ISO26262

Nominal Function

NEW VULNERABILITY OR SOFTWARE UPDATE =

RE-DESIGN

RE-VERIFY

Nominal Function

Functional Safety ISO26262

Vehicle Cybersecurity ISO/SAE21434

Define Security Goals | Design Safety Goals | Design Function | Verify/Validate Function | Validate Safety Goals | Validate Security Goals

Design Functional Security Concept | Design Functional Safety Concept | Design Architecture | Verify Architecture | Verify Functional Safety Concept | Verify Functional Security Concept

Design Technical Security Concept | Design Technical Safety Concept | Design System | Verify System | Verify Technical Safety Concept | Verify Technical Security Concept

Define Component SW & HW Security Requirements | Define Component SW & HW Safety Requirements | Design Component SW & HW | Verify Component SW & HW | Verify Component SW & HW Safety Requirements | Verify Component SW & HW Security Requirements

Automaker & Supplier Create HW & SW Solution

Supplier Defines Additional Technical Security Requirements

BH.

TARA-as-a-Service

How we work

Item Definition

Documentation

A Block Harbor security analyst will review documentation provided by the customer on technical details and functionsof the target item. Then, we'll document assets relevant for cybersecurity in a formal item definition to perform a security analysis against.

Item Owner Review

Block Harbor will set up an interview with the item owner to refine the item definition and ensure accuracy before performing the security analysis.

Security Objectives

Then, we'll work with the customer to understand the security objectives of the item so that we don't miss critical considerations that we may not be accounting for.

Security Analysis

Damage Scenarios

Our security experts will document damage scenarios based on their understand of the target item. Damage scenarios used Safety, Financial, Operational, and Privacy dimensions to compute an impact level.

Threat Scenarios

Block Harbor's team identifies possible threat scenarios to realize the damage scenarios and violate the security objectives of the item. Threat scenarios use attack feasibility level to determine the likelihood of the scenario.

Risk and Risk Treatments

Block Harbor will generate a set of risks based on the security analysis that the target item faces. Then, we'll work with the item owner to identify security controls that can be used to treat the risks.

Why Block Harbor?

Block Harbor was founded in 2014 in Detroit providing services to automakers and automotive suppliers to keep vehicles safe, ranging from penetration testing to running a 24/7/365 Security Operation Center (SOC). We're on a mission to build great solutions to keep mobility safe.

- Vehicle Cybersecurity Labs
  - -Penetration Testing
  - -Fuzzing
  - -V&V-as-a-Service
  - -Vehicle Cybersecurity Lab Buildout
- Vehicle Security Operations
  - -Vehicle Security Operation Center (VSOC)
  - -Threat Analysis and Risk Assessment (TARA)
  - -Vehicle Cybersecurity Management System (CSMS)
- Vehicle Cybersecurity Consulting

Block Harbor. Cybersecurity

To learn more about working with our team to meet your vehicle security needs, please visit blockharbor.io