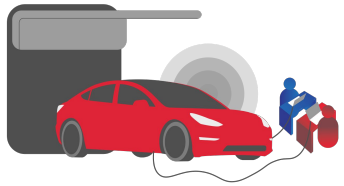
Block Harbor.
Cybersecurity

Threat Analysis and Risk Assessment (TARA) Service

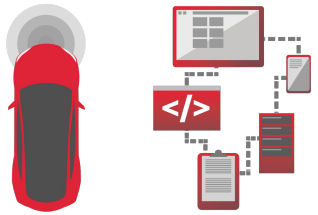
Block Harbor. Services



Vehicle Cybersecurity Labs (Red Team)

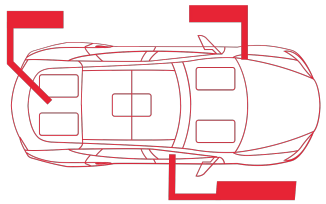
Vehicle/Subsystem/Component Penetration Testing
Vehicle/Subsystem/Component Fuzzing
Verification/Validation-as-a-Service (VaaS)

Vehicle Cybersecurity Lab Buildout



Vehicle Security Operations (Blue Team)

Vehicle Security Operation Center (VSOC)
Vehicle/Subsystem/Component Threat Analysis & Risk Assessment (TARA)
Vehicle Cybersecurity Management System (CSMS)
Security Concept Design
SW or HW Security Requirements Definition



Vehicle Cybersecurity Consulting

ISO/SAE 21434, WP.29, TISAX, & more

Training, Upskilling, Manual Creation

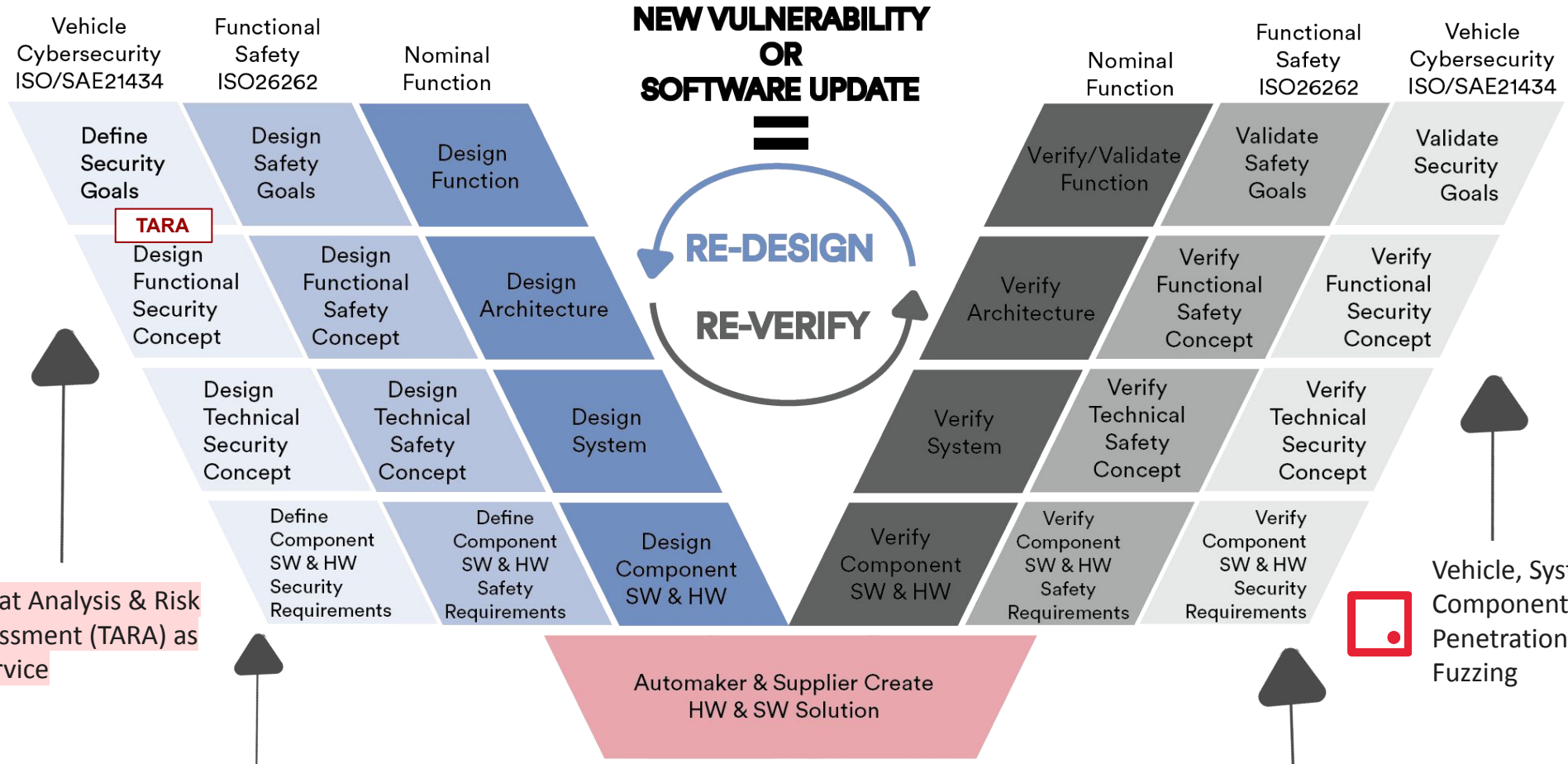
Process Design & Product Design

Some of our great customers.

Ford
DANA
VOLVO TRUCKS
DENSO
DANLAW
STELLANTIS
GENTHERM
LORDSTOWN
LOCOMATION
BorgWarner
Togg

est. 2014 in Detroit.

BH.



Threat Analysis & Risk Assessment (TARA) as a Service

Training
Process Design
Product Design

Security Concept Design
SW Security Requirements Definition
HW Security Requirements Definition

Verification & Validation as a Service

Vehicle, System, and Component Penetration Testing & Fuzzing

Vehicle Cybersecurity Lab Buildout

Vehicle Cybersecurity Management System (CSMS)

Vehicle Cybersecurity Consulting: ISO/SAE 21434, UNECE WP.29, & more

Vehicle Security Operation Center

Training
Process Design
Product Design

Unlocking Value Together.

Experience and Expertise:

- Conducted over **300** Threat Analysis and Risk Assessments (TARAs) across vehicle, system, and component levels
- Collaboration with diverse major OEMs and their Tier One suppliers showcases our proficiency
- Hands-on experience translates to unmatched insights and recommendations for safeguarding the automotive ecosystem

Client-Centric Approach, Success Looks Like:

- Communication: Weekly to bi-weekly TARA status (e.g. Status Meetings)
- Utilizing a customer issue tracking platform i.e Jira for visibility on project status
- Our shared timetable provides real-time tracking and visibility into every stage of the TARA process.
- Beyond TARA, we remain accessible and responsive to your questions and concerns
- Please share with us your vision of a successful engagement, and we'll customize our services to align with your needs.

BH.

VSO-TARA Service Offerings. Blue Team

Threat Analysis & Risk Assessments (TARA)

★ Starting from $45,000

★ Timeline

4 - 12 weeks

When to Consider?

- Support for UN R 155 & ISO/SAE 21434
- When Introducing New Features or Technologies
- During the Early Stages of Product Development

Entails:

- Component, system and/or vehicle level TARA compliant with ISO/SAE 21434
- Attack path analysis
- Identify and develop security goals
- Support for risk treatment decisions

TARA Review

★ Starting from $7,500 per TARA

★ Timeline

2 to 4 weeks +

When to Consider?

- Requiring an expert review to ensure their TARA meets industry standards and best practices.
- Wanting to leverage professional expertise to identify gaps or risks that might have been overlooked
- Preparing for audits or certifications and wanting assurance in their TARA's quality

Entails:

- VSEC Platform Access and TARA Upload
- Preliminary Review by User
- In-Depth Review by Expert Team
- Final Reporting on findings

Cybersecurity Concept

★ Starting from $12,000

★ Timeline

2 weeks+

When to Consider?

- Generation of a new TARA
- When Updating or Revising an Existing Product
- At the Start of a New Vehicle or System Development

Entails:

- WP-09-03 Cybersecurity Goals
- WP-09-04 Cybersecurity Claims

BH.

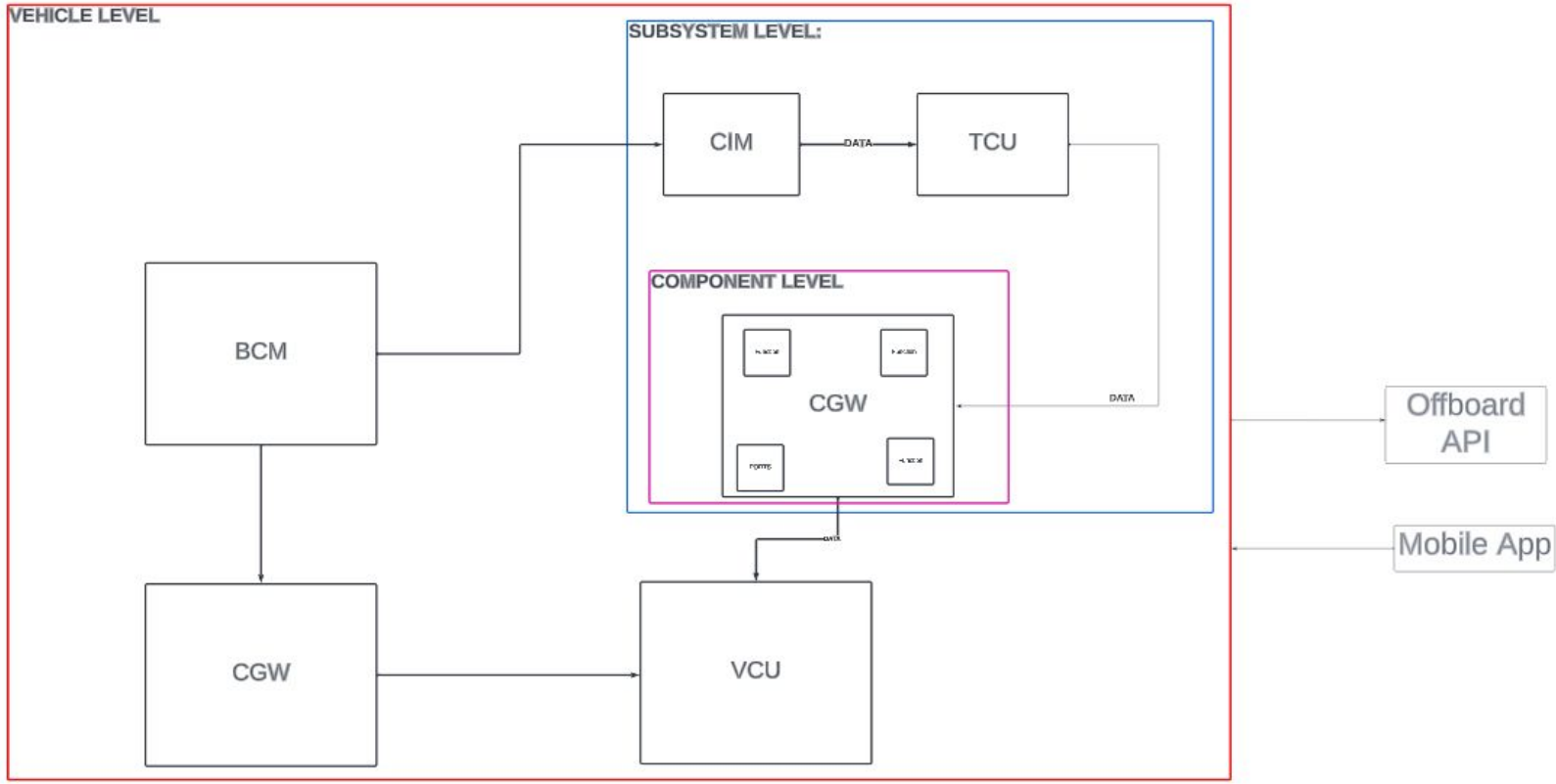
TARAs & TARA Reviews at Each Level

Vehicle
Full E/E Architecture

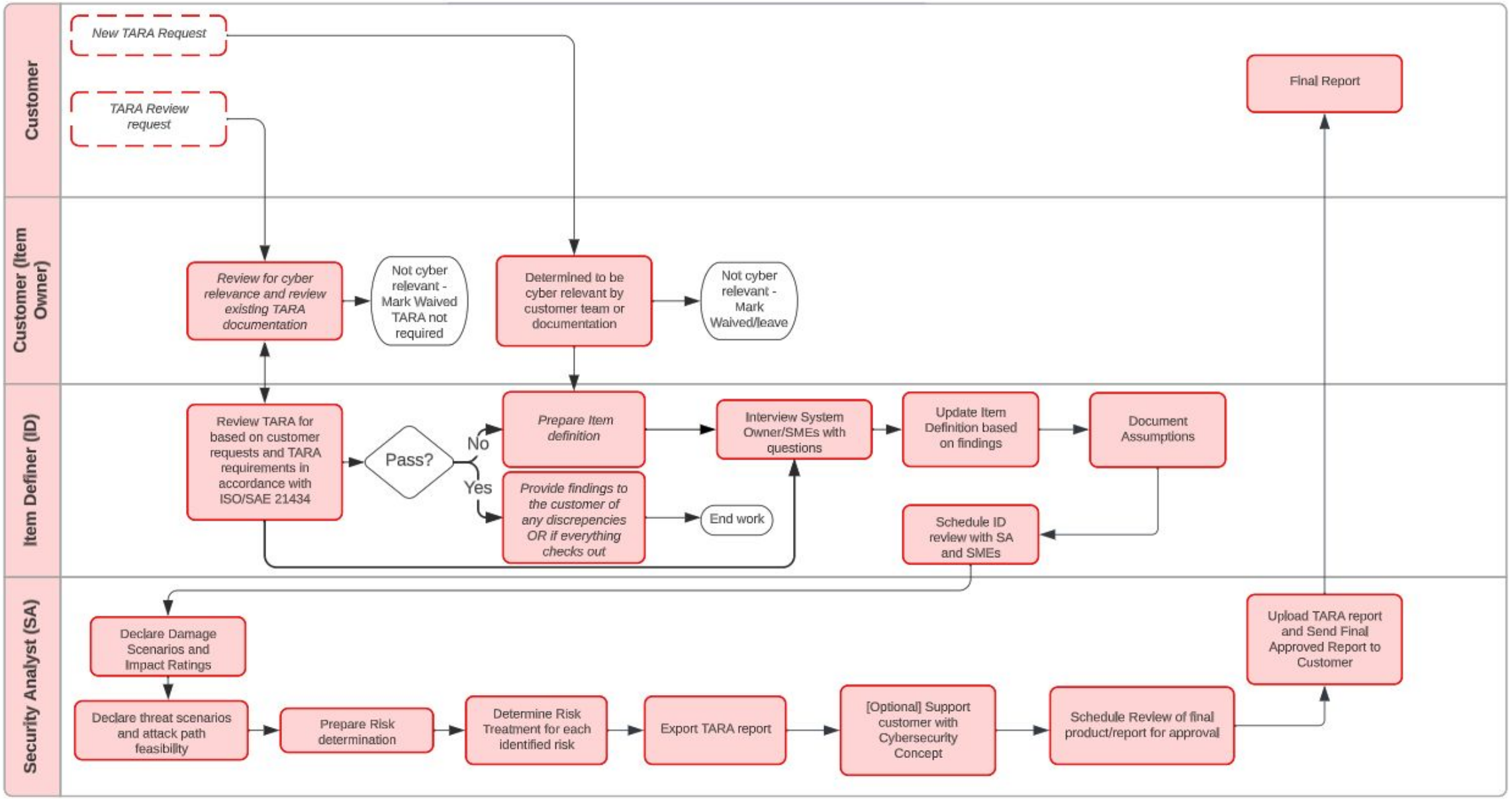
System
Feature Level / Subsystem Level

Component
ECU

Chip Level



Block Harbor - TARA Engagement Overview



*The Item Definer and the Security Analyst can be the same individuals. But we do heavily rely on the customer to provide us with accurate information as our analysis will be against what has been defined in the Item Definition

Mid Engagement we send the customer a TARA draft report for alignment.

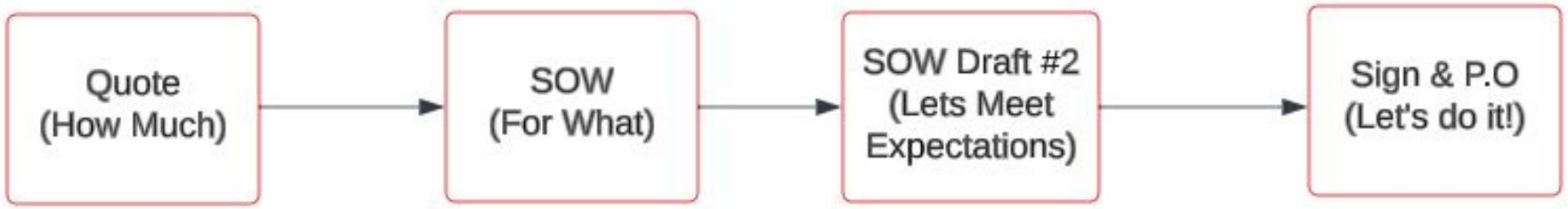
High Level TARA Methodology.

Step 1	Define the perimeter **Clause Ref #: 9.3**	The item definition [WP-09-01] provides details regarding the context in which the asset exists, operates, and can be compromised due to misuse of the product. In this step, declare elements: Components, Channels, Data, Data Flows.
Step 2	Define the assets of the Item **Clause Ref #: 15.3**	Relevant assets within scope. This can be: Components, Channels, Data, Data Flows.
Step 3	Define Damage Scenarios and Impact Ratings **Clause Ref #: 15.5**	Damage scenarios [WP-15-01 & WP-15-02] with Impact ratings [WP-15-04] based on Safety, Financial, Operational, and Privacy (SFOP) damages
Step 4	Define the threat scenarios **Clause Ref #: 15.4**	Threat Scenarios [WP-15-03] Identified using Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation Privilege (STRIDE)
Step 5	Create Attack Paths for each threat scenario and determine attack feasibility **Clause Ref #: 15.6 & 15.7**	Creating attack trees consisting of attack paths [WP-15-05]; that realize the threat scenaiors. Attack feasibility ratings [WP-15-06] based on Elapsed Time, Special Expertise, Knowledge of Item, Window of Opportunity, and Equipment.
Step 6	Define the Risk Value **Clause Ref #: 15.8**	Risk value [WP-15-07] determined by the cumulative risk rating according to the worst-case potential Impact and Feasibility
Step 7	Risk Treatment Decision **Clause Ref #: 15.9**	For each threat scenario, considering its risk values [WP-15-07], one or more risk treatment option(s) are determined [WP-15-08]

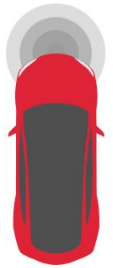
Note: The depth at which we delve into attack tree paths during the TARA is contingent on the phase at which the assessment is being conducted. If an attack tree methodology is requested collaboration with the customer's Subject Matter Expert (SME) team would be required for a more detailed exploration. Otherwise, our focus remains on providing high-level descriptions of the threats posed to the item.

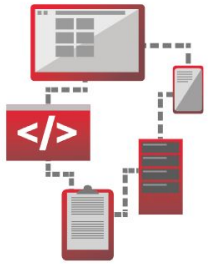
BH.

Next Steps…


Quote
(How Much)
SOW
(For What)
SOW Draft #2
(Lets Meet
Expectations)
Sign & P.O
(Let's do it!)

Working Together.





What else do we offer?

Service	Description
TARA	We can conduct a Threat Analysis and Risk assessment and provide you with a detailed report. One to one mapping to each work product in ISO/SAE 21434.
Cybersecurity Concept	Support the cybersecurity concept phase to help consumers identify cyber security goals and cybersecurity requirements.
TARA Review	We can review and audit an already existing TARA
Instructor led TARA Training	One weeTARA training workshop with an Instructor
TARA Training Material	We can provide you with material which you can use for your in-house training
VSEC for TARA	Use our platform (VSEC) for on-demand and self-paced TARA training. Customized to meet your organizations needs.
Risk Manager	Use our block **Risk Manager** within our platform (VSEC) for TARA and cybersecurity concept generation

BH.

TARA vs Threat Model.

Threat Modeling.

- Definition:
  - A structured approach to identifying, describing, and analyzing security threats and attack vectors to inform security measures.
- Objectives of Threat Modeling:
  - To understand the threat landscape, identify potential vulnerabilities, and inform risk assessment and mitigation measures.
- Core components of Threat Modeling:
  1. Identifying threats and attack vectors: Understanding the different ways attackers could potentially exploit the system.
  2. Analyzing security threats: Assessing the likelihood and impact of different threats.
  3. Constructing attack trees: Visualizing the different paths an attacker could take to exploit vulnerabilities in the system.

Note: Threat Modeling does not include a **risk assessment.**

Threat Analysis and Risk Assessment.

(TARA goes into further steps)

- Definition:
  - A method to evaluate cybersecurity risks within a product or system, encompassing system modeling, asset identification, attack modeling, and assessing the consequences of attacks.
- Objectives:
  - To identify potential threats and risks, and develop appropriate protective measures to mitigate these risks.
- Key steps in TARA:
  1. Threat modeling: Creating a model to understand the system architecture and flow of information.
  2. Asset identification: Identifying critical assets that need protection.
  3. Threat/Attack modeling: Identifying potential attack vectors and how they could impact the system.
  4. Assessing the consequences of attacks: Evaluating the potential impact and severity of different attack scenarios.
  5. Risk value determination: Determining risk based on impact and feasibility of the threat and corresponding damage scenarios
  6. Risk Treatment determination: Avoid, reduce, share, or retain the risk

Comparative Analysis.

- Distinction between TARA and Threat Modeling:
  - TARA is a broader process that encompasses threat modeling among other steps to systematically evaluate cybersecurity risks. Threat modeling is narrowly focused on identifying and analyzing the threat landscape and attack vectors.
- How Threat Modeling informs TARA:
  - By identifying and analyzing potential threats, threat modeling provides essential input for the TARA process, aiding in a comprehensive risk assessment.
- Integration of both processes in cybersecurity risk management:
  - Both processes complement each other and form integral parts of the cybersecurity risk management framework as outlined in the ISO/SAE 21434 standard.

TARA borrows its structure from functional safety's Hazard Analysis and Risk Assessment (HARA)

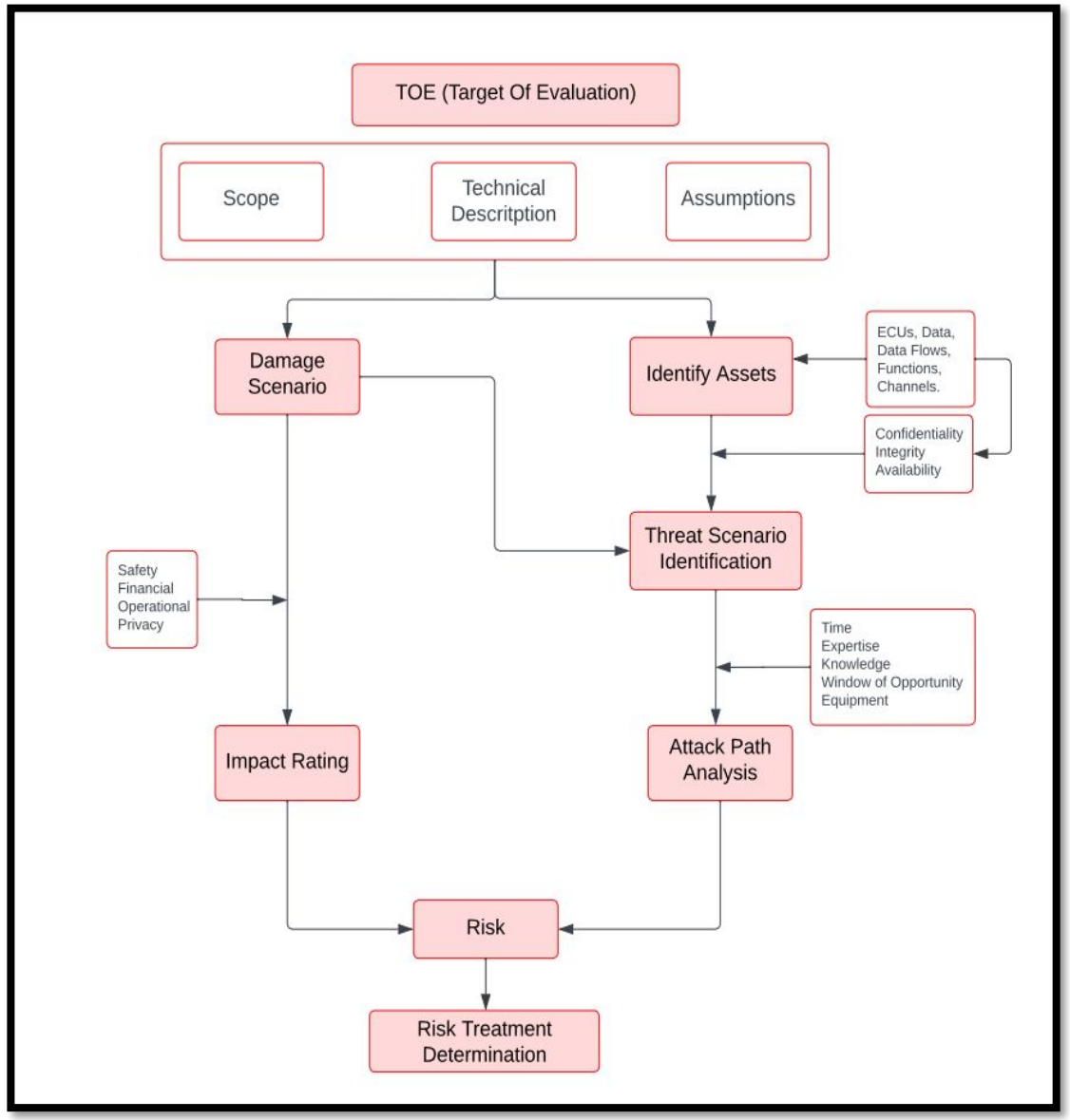
TARA vs HARA.

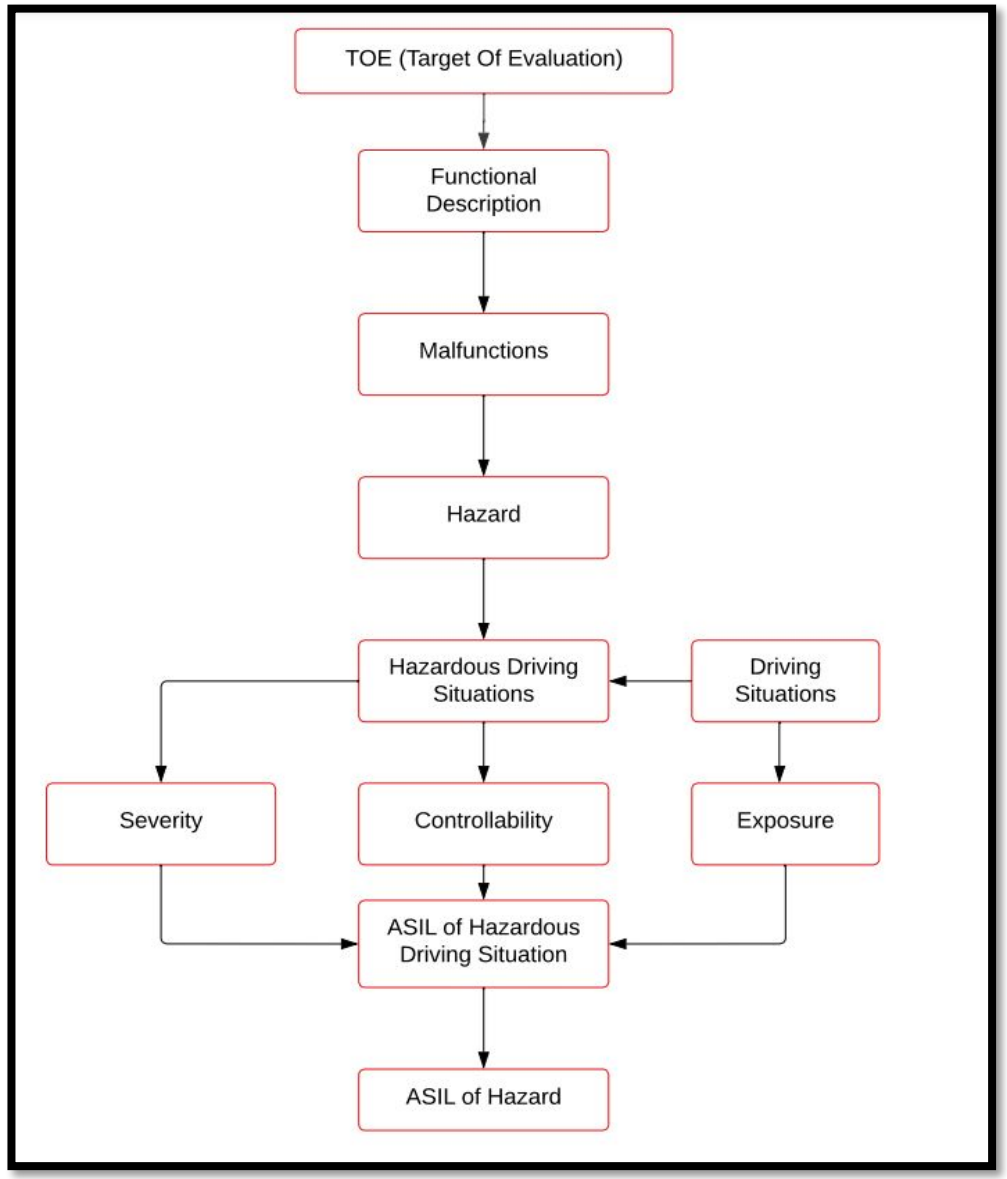
Scope:

- TARA: focused on identifying potential threats and cybersecurity risks, and develop appropriate protective measures to mitigate these risks.

- HARA: focuses on identifying and assessing risks related to functional safety. It aims to ensure that automotive systems and components are free of unreasonable risk due to hazards caused by malfunctioning behavior in a specific use-case scenario.

TARA vs HARA


TOE (Target Of Evaluation)
Scope
Technical Descritption
Assumptions
Damage Scenario
Identify Assets
ECUs, Data, Data Flows, Functions, Channels.
Confidentiality Integrity Availability
Threat Scenario Identification
Safety Financial Operational Privacy
Time Expertise Knowledge Window of Opportunity Equipment
Impact Rating
Attack Path Analysis
Risk
Risk Treatment Determination


TOE (Target Of Evaluation)
Functional Description
Malfunctions
Hazard
Hazardous Driving Situations
Driving Situations
Severity
Controllability
Exposure
ASIL of Hazardous Driving Situation
ASIL of Hazard

Understanding Threat Model vs. TARA.

- Threat Model: Like a blueprint of your security "house" that reveals vulnerabilities and attack points.
- Metaphor: Think of it as understanding your house's structure, including doors and windows.
- TARA - Threat and Risk Assessment: Goes further by systematically analyzing how those threat scenarios can be exploited to achieve damage scenarios, including the prioritization of those risks.
- Metaphor: It's like exploring how your front door could be broken into.
- Connection: Threat Model identifies issues, and TARA solves them systematically.
- Key Message: Working together to fortify security.

Let's Secure Your Future Together.

Building great solutions to keep mobility safe.

BH.

contactus@blockharbor.io