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.
inally, 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 .

{SOLUTION POINT 2}

{Sub Point 2}

Our security experts will then run the vulnerabilities through test cases to canvas the internal attack surface laterally. As the internal attack surface expands during testing, the client and stakeholders are informed on a cyclic basis.

{Sub Point 2}

The findings of the engagement are encapsulated in a document in order to help visualize the attack surfaces that need to be hardened or refactored. The report will consist of exploitation points of concepts, processes, remediation plans, and assessment of risk.

How we work

{SOLUTION POINT 1}

{Sub Point 1}

After vehicle, system, or component cybersecurity design is complete, implemented, and functionally tested, penetration testing tests that the cybersecurity goals were actually achieved.

{Sub Point 2}

Once the target has been canvassed, the next step is to identify low-hanging fruit. Using our suite of tools, we readily probe for vulnerabilities and vectors of attack.

{SOLUTION POINT 2}

{Sub Point 2}

Our security experts will then run the vulnerabilities through test cases to canvas the internal attack surface laterally. As the internal attack surface expands during testing, the client and stakeholders are informed on a cyclic basis.

{Sub Point 2}

The findings of the engagement are encapsulated in a document in order to help visualize the attack surfaces that need to be hardened or refactored. The report will consist of exploitation points of concepts, processes, remediation plans, and assessment of risk.

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.

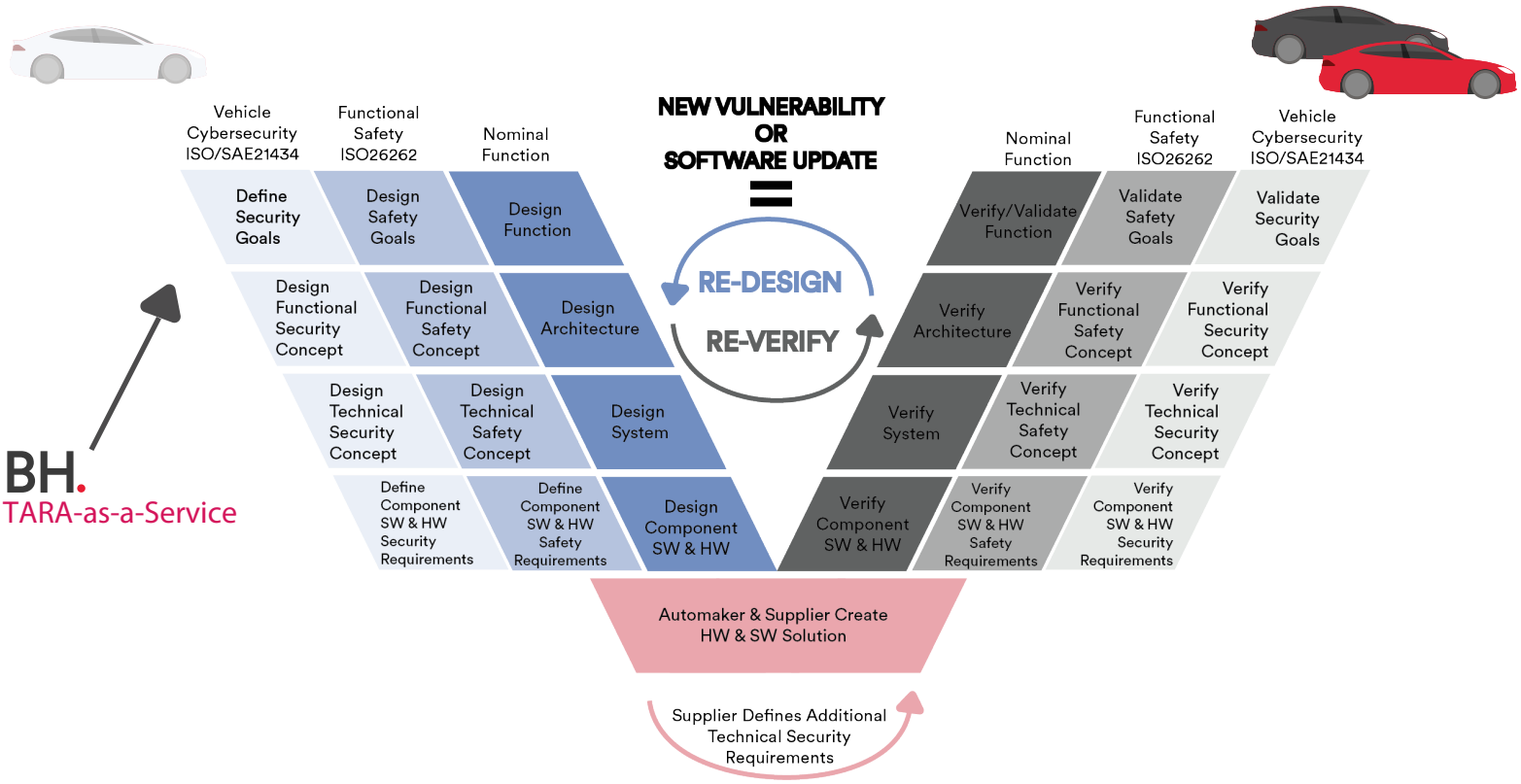
- Cybersecurity Assessments
  - -TARA-as-a-Service
  - -Pentration Testing
- Managed Cybersecurity Services
  - -Fuzzing-as-a-Service
  - -Verification/Validation-as-a-Service
  - -Vulnerability Management
- Cybersecurity Consulting
  - -ISO/SAE 21434 Consulting
  - -UNR155 Consulting

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.



Solution In Depth

{SOLUTION POINT 2}

{Sub Point 2}

Our security experts will then run the vulnerabilities through test cases to canvas the internal attack surface laterally. As the internal attack surface expands during testing, the client and stakeholders are informed on a cyclic basis.

{Sub Point 2}

The findings of the engagement are encapsulated in a document in order to help visualize the attack surfaces that need to be hardened or refactored. The report will consist of exploitation points of concepts, processes, remediation plans, and assessment of risk.

{SOLUTION POINT 2}

{Sub Point 2}

Our security experts will then run the vulnerabilities through test cases to canvas the internal attack surface laterally. As the internal attack surface expands during testing, the client and stakeholders are informed on a cyclic basis.

{Sub Point 2}

The findings of the engagement are encapsulated in a document in order to help visualize the attack surfaces that need to be hardened or refactored. The report will consist of exploitation points of concepts, processes, remediation plans, and assessment of risk.

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.

- Cybersecurity Assessments
  - -TARA-as-a-Service
  - -Pentration Testing
- Managed Cybersecurity Services
  - -Fuzzing-as-a-Service
  - -Verification/Validation-as-a-Service
  - -Vulnerability Management
- Cybersecurity Consulting
  - -ISO/SAE 21434 Consulting
  - -UNR155 Consulting

Block Harbor. Cybersecurity

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